DYNAMIX UM-A

ADSL Router
4/1 Port

User's Manual

Copyright

Copyright © 2002 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

Disclaimer

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a residential environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment ON and OFF, the user is encouraged to try to reduce the interference by one or more of the following measures:

- Adjust or relocate the receiving antenna
- Increase the separation between the equipment or device
- Consult a dealer or an experienced technician for assistance

CE Declaration of Conformity

This is to certify that this device complies the essential protection requirements of the European Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22). Compliance with the applicable regulations is dependent upon the use of shielded cables. It is the responsibility of the user to procure the appropriate cables.

Contents

Chapter 1 : Introduction 6

1.1 Four Port ADSL Router ***7***

1.1.1 Features 7

1.2 One Port ADSL Router ***10***

1.2.1 Features 10

1.3 Scope ***13***

1.4 Audience ***14***

1.5 Document Structure ***15***

1.6 System Requirement ***16***

Chapter 2 : Getting To Know Your ADSL Router 17

2.1 For Four Port ADSL Router ***17***

2.1.1 Back Panel 17

2.1.2 Front Panel 18

2.1.3 Connection Mechanism 19

2.2 For One Port ADSL Router ***21***

2.2.1 Back Panel 21

2.2.2 Front Panel 22

2.2.3 Connection Mechanism 23

Chapter 3. Administrator's Computer Setting 25

3.1 Windows 98/ME ***26***

3.2 Windows 2000 ..... ***27***

3.3 Windows XP ***28***

Chapter 4. Device Administration 29

4.1 Login ***29***

4.2 Quick Setup ***31***

4.2.1 Quick Setup : Automatic Setting 32

4.2.2 Quick Setup : Manual Setup 35

4.3 Advanced Mode 40
4.3.1 Advanced Setup—Status 41
4.3.1.1 Status – Main Status 42
4.3.1.2 Status – PPP 44
4.3.1.3 Status – ADSL 46
4.3.2 Advanced Setup — Configuration 48
4.3.2.1 Configuration—WAN 49
4.3.2.2 Configuration—LAN 57
4.3.2.3 Configuration—PPP 60
4.3.2.4 Configuration—NAT 67
4.3.2.5 Configuration – Virtual Server 69
4.3.2.6 Configuration – Bridge Filtering 71
4.3.2.7 Configuration—DNS 73
4.3.2.8 Configuration – User Password Configuration 75
4.3.2.9 Configuration – Save Setting/Reboot 76
4.3.3 Advanced Setup – Admin Privilege 77
4.3.3.1 Admin Privilege – WAN Status 78
4.3.3.2 Admin Privilege – ATM Status 79
4.3.3.3 Admin Privilege – ADSL Configuration 80
4.3.3.4 Admin Privilege – Route Table 81
4.3.3.5 Admin Privilege – Learned MAC Table 83
4.3.3.6 Admin Privilege – RIP Configuration 84
4.3.3.7 Admin Privilege – Misc Configuration 87
4.3.3.8 Admin Privilege – TCP Status 91
4.3.3.9 Admin Privilege – Admin Password Configuration 92
4.3.3.10 Admin Privilege – Reset To Factory Default 93
4.3.3.11 Admin Privilege – Diagnostic Test 94
4.3.3.12 Admin Privilege – System Log 98
4.3.3.13 Admin Privilege – Local Code Image Update 99
4.3.3.14 Admin Privilege – Network Firmware Image Update 100
4.3.3.15 Admin Privilege – Boot Code Image Update 101
4.3.3.16 Admin Privilege – Firewall 102
4.3.3.16.1.1 Advanced Options – Protection Policy 103
4.3.3.16.1.2 Advanced Options – Hacker Log 105
4.3.3.16.1.3 Advanced Options – Service Filtering 106
4.3.3.16.2.1 Firewall Databases – IP Group 107
4.3.3.16.2.2 Firewall Databases – Service Group 108
4.3.3.16.2.3 Firewall Databases – Time Window 109
4.3.3.16.3.1 Inbound/Outbound Policies – Inbound Policy 110

4.3.3.16.3.2 Inbound/Outbound Policies – Outbound Policy 114
4.3.4 Advanced Mode – Manage Public Servers 120
4.4 Status ***122***
4.4.1 Status – Current Setting 122
4.4.2 Status – System Log 123
Appendix A : Network Address Translation **125**
A.1 Basic NAT ***126***
A.2 Static NAPT ***127***
A.3 Functional Descriptions ***128***
A.3.1 Outbound Access 129
A.3.2 Inbound Access 131
Appendix B Frequently Asked Questions **132**
Appendix C Troubleshooting Guide **135**
Appendix D Network Setup Guide **136**
D.1 Windows XP/2000 ..... ***136***
D.2 Windows 95/98/98SE/Me ***137***
D.3 AC OS (7.6.1 or higher) ***138***
D.4 MAC OS X ***139***
Appendix E Common Error Messages **140**
Appendix F Glossary **141**

Chapter 1 : Introduction

Congratulations on your purchase of this outstanding ADSL Router.

ADSL is a transmission technology used to carry user data over a single twisted-pair line between the Central Office and the Customer Premises. The downstream data rates can go up to 8 Mbps. The upstream data rates can go up to 1Mbps. This asymmetric nature lends itself to applications such as Internet access and video delivery.

ADSL Router is a Four/One Port Ethernet ADSL Router combines an “Always-On” high speed Asymmetric Digital Subscriber Line (ADSL) connection to the Telephone Line, and 10/100BASE-T Ethernet Switch connection to a host PC or other Ethernet device to enable the widest array of host connectivity.

This Ethernet ADSL Router device set is fully compliant with ANSI T1.413 Issue 2, ITU G.992.1 and ITU G.992.2 specification. This rate-adaptive solution is especially designed for Customer Premise Equipment that supports downstream data rates up to 8 Mbps and upstream data rates up to 1 Mbps.

With minimum setup, you can install and use the router within minutes.

1.1 Four Port ADSL Router

1.1.1 Features

- **The Four Port ADSL Router provides the following features:**
  - Full rate ANSI T1.413 Issue 2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
  - Fully compliant with Annex A/B/B (U-R2) ADSL specifications.
  - Downstream and Upstream data rates up to 8Mbps and 1Mbps.
  - PPPoE/PPP protocol for dial-up ADSL service.
  - Support Firewall functionality.
  - Support UPnP (Universal Plug-and-Play) specifications (Optional).
  - Web-based setup for installation and management.
  - Built in 4*10/100 Mbps Switch port for LAN connection.
  - Compliant with IEEE 802.3/802.3u and auto-negotiation.
  - Support full-duplex 802.3 flow control.
  - Support packet filtering functionality.
  - Flash memory for firmware upgrade.
  - Hardware Reset button for fast default setting recovery.
  - LEDs indicator indicates connection status.

- **ADSL Standards**
  - Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
  - Downstream and Upstream data rates up to 8Mbps and 1Mbps.
  - Support Dying Gasp functionality.

- **ATM Protocols**
  - Support PPPoA (RFC2364).
  - Support PPPoE (RFC2516).
  - Router/Bridged Ethernet over ATM (RFC1483).
  - Classical IP over ATM (RFC1577).
  - ATM Forum UNI 3.1/4.0 PVC, ATM SAR, ATM AAL5 and OFM F4/F5.
  - Support up to 8PVCs.

- **Router Mode**
  - IP Routing – RIPv1 and RIPv2.
  - Static Routing.
  - DHCP Server and Client.
  - Support DNS proxy.
  - Support NAT and NAPT functionality.
  - Support IPSec, L2TP, PPTP Pass-Through.
  - Support ICMP and IGMP.

- **Firewall**
  - Statefull Packet Inspection (SPI).
  - DoS (Denial of Service) protection.
  - Service Filtering.
  - Access Policies based on IP Address, Service Group, Time, Inbound/Outbound Policy.
  - Hacker Log.

- **Ethernet Standards**
  - Built-in 4 Port 10/100Mbps Ethernet Switch which compliant with IEEE 802.3x standards
  - Automatic MDI/MDI-X crossover for 10/100Base-T/port.

- **Web-Based Management**
  - Firmware upgrade via FTP.
  - WAN and LAN connection statistics.
  - Configuration of static routes and routing table, NAT/NAPT and VCs.
  - PPP user ID and password.

- **Security Support**
  - Hidden by NAT. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users out-side the LAN from finding and directly accessing the PCs on the LAN.
  - Port Forwarding with NAT. The 4 Port ADSL Router allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated "DMZ" host computer. Forwarding of single ports or ranges of ports are configurable.
  - Support URL Blocking. Prevent any LAN clients from accessing specific Internet site by set- ting the URL keywords. The 4 Port ADSL Router will reject all those web site whose URL names are matched or partially matched with the keywords.
  - Support MAC Filtering function. This function enable the administrator to control the LAN client computers to access the Internet by the hardware MAC Address.

- **Content Filtering**
  - Blocks unwanted traffic from the Internet to your LAN.
  - Blocks access from your LAN to Internet locations or services that you'd specified.
  - Logs security incidents. The 4 Port ADSL Router will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins.

- **Extensive Protocol Support**
  - IP Address Sharing by NAT. The 4 Port ADSL Router allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP).
  - Automatic Configuration of DHCP. The 4 Port ADSL Router dynamically assigns network configuration information, including IP Address, WAN Gateway, Domain Name Server (DNS) Addresses, … etc. This greatly simplifies configuration of PCs on your local network.
  - Dynamic DNS. This is a method of keeping a domain name linked to a changing IP Address as not all computers use Static IP addresses. Typically, when a user connects to the Internet, the user's ISP assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of that specific connection.

- PPP over Ethernet (PPPoE). PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.
- PPTP (Point-to-Point Tunneling Protocol) – PPTP is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private " Tunnels " over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network.

➢ **Easy Installation and Management**

- Quick Setup. The Quick Setup is meant to help you install the product quickly and easily.
- Browser-based management. Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh or Linux.
- Visual monitoring. The 4 Port ADSL Router's front panel's LEDs provide an easy way to monitor the connection status and activity.

1.2 One Port ADSL Router

1.2.1 Features

- **The One Port ADSL Router provides the following features:**
  - Full rate ANSI T1.413 Issue 2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
  - Fully compliant with Annex A/B/B (U-R2) ADSL specifications.
  - Downstream and Upstream data rates up to 8Mbps and 1Mbps.
  - PPPoE/PPP protocol for dial-up ADSL service.
  - Support Firewall functionality.
  - Support UPnP (Universal Plug-and-Play) specifications (Optional).
  - Web-based setup for installation and management.
  - Support packet filtering functionality.
  - Flash memory for firmware upgrade.
  - Hardware Reset button for fast default setting recovery.
  - LEDs indicator indicates connection status.

- **ADSL Standards**
  - Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
  - Downstream and Upstream data rates up to 8Mbps and 1Mbps.
  - Support Dying Gasp functionality.

- **ATM Protocols**
  - Support PPPoA (RFC2364).
  - Support PPPoE (RFC2516).
  - Router/Bridged Ethernet over ATM (RFC1483).
  - Classical IP over ATM (RFC1577).
  - ATM Forum UNI 3.1/4.0 PVC, ATM SAR, ATM AAL5 and OFM F4/F5.
  - Support up to 8PVCs.

- **Router Mode**
  - IP Routing – RIPv1 and RIPv2.
  - Static Routing.
  - DHCP Server and Client.
  - Support DNS proxy.
  - Support NAT and NAPT functionality.
  - Support IPSec, L2TP, PPTP Pass-Through.
  - Support ICMP and IGMP.

- **Firewall**
  - Statefull Packet Inspection (SPI).
  - DoS (Denial of Service) protection.
  - Service Filtering.
  - Access Policies based on IP Address, Service Group, Time, Inbound/Outbound Policy.
  - Hacker Log.

- **Web-Based Management**
  - Firmware upgrade via FTP.
  - WAN and LAN connection statistics.

- Configuration of static routes and routing table, NAT/NAPT and VCs.
- PPP user ID and password.

- **Security Support**
  - Hidden by NAT. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users out-side the LAN from finding and directly accessing the PCs on the LAN.
  - Port Forwarding with NAT. The 1 Port ADSL Router allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated “DMZ” host computer. Forwarding of single ports or ranges of ports are configurable.
  - Support URL Blocking. Prevent any LAN clients from accessing specific Internet site by set- ting the URL keywords. The 1 Port ADSL Router will reject all those web site whose URL names are matched or partially matched with the keywords.
  - Support MAC Filtering function. This function enable the administrator to control the LAN client computers to access the Internet by the hardware MAC Address.

- **Content Filtering**
  - Blocks unwanted traffic from the Internet to your LAN.
  - Blocks access from your LAN to Internet locations or services that you’d specified.
  - Logs security incidents. The 1 Port ADSL Router will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins.

- **Extensive Protocol Support**
  - IP Address Sharing by NAT. The 1 Port ADSL Router allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP).
  - Automatic Configuration of DHCP. The 1 Port ADSL Router dynamically assigns network configuration information, including IP Address, WAN Gateway, Domain Name Server (DNS) Addresses, … etc. This greatly simplifies configuration of PCs on your local network.
  - Dynamic DNS. This is a method of keeping a domain name linked to a changing IP Address as not all computers use Static IP addresses. Typically, when a user connects to the Internet, the user's ISP assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of that specific connection.
  - PPP over Ethernet (PPPoE). PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.
  - PPTP (Point-to-Point Tunneling Protocol) – PPTP is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private " Tunnels " over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network.

- **Easy Installation and Management**
  - Quick Setup. The Quick Setup is meant to help you install the product quickly and easily.
  - Browser-based management. Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh or Linux.
  - Visual monitoring. The 1 Port ADSL Router's front panel's LEDs provide an easy way to monitor the connection status and activity.

1.3 Scope

This document provides the descriptions and usages for the **ADSL Router**'s Web pages that are used in the configuration and setting process. Both basic and advanced descriptions and concepts are discussed. To help the reader understand more about these Web pages, some questions and answers (Q&A) are appended after the definition of each Web page along with the appendices at the end of the guide.

1.4 Audience

This document is prepared for use by those customers who purchasing **ADSL ROUTER** and using the firmware. It assumes the reader has a basic knowledge of ADSL and networking.

1.5 Document Structure

Chapter 1: Introduction, provides a brief introduction to the product and user guide.

Chapter 2: Getting to know your ADSL Router, provides device specifications and hardware connection mechanism.

Chapter 3: Administrator's computer setting, provides Windows system Network's configurations.

Chapter 4: Device Administrator, describes the pages found under the Configuration menu. These pages allow the user to view, update, and save the **ADSL ROUTER** configurations.

Appendix A: Network Address Translation, provides an introduction to Network Address Translation (NAT).

Appendix B: Frequently Asked Questions, is a compilation of useful questions regarding ADSL Router setup.

Appendix C: Troubleshooting Guide, is a compilation of questions and answers relating to common problems dealing with Windows Networking and the **ADSL ROUTER** Configuration.

Appendix D: Network Setup Guide, provides additional support on setting up Windows and Mac OS networks.

Appendix E: Common Error Messages, provides an explanation and solution of some common error messages that may occur while configuring the **ADSL ROUTER**.

Appendix F: Glossary, provides definitions of terms and acronyms.

1.6 System Requirement

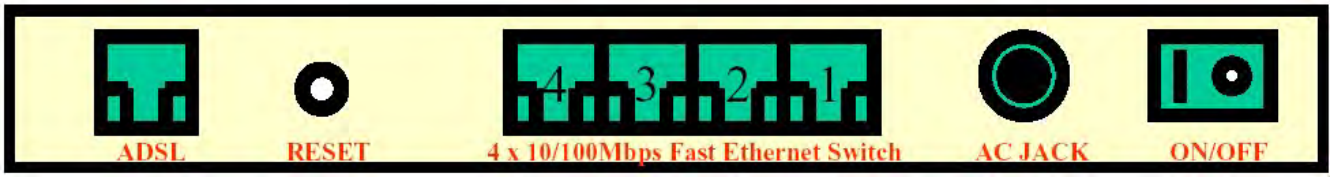
- Personal computer (PC)
- Pentium II compatible processor and above
- Internet Browser
- 64 MB RAM or more
- 50 MB of free disk space minimum
- Ethernet Network Interface Controller (NIC) RJ45 Port
- Ethernet (CAT5) Cable
- Power adaptor for ADSL Router
- CD-ROM drive

Chapter 2 : Getting To Know Your ADSL Router

2.1 For Four Port ADSL Router

2.1.1 Back Panel

The back panel of the 4 Port ADSL Router contains WAN/LAN Connection, USB Port Connection and Power Switch.

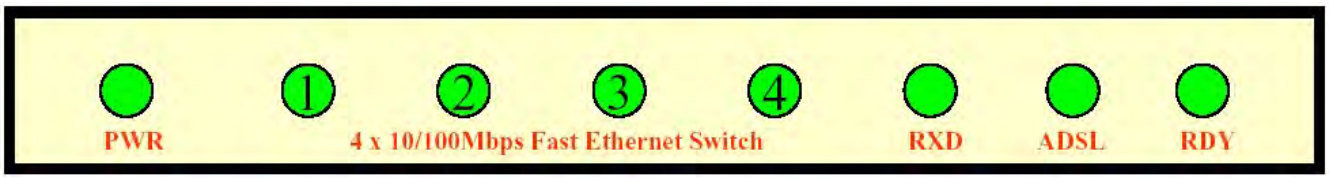


ADSL	Port for connecting the 4 Port ADSL Router to the ADSL Service Provider.
RESET	Restore the 4 Port ADSL Router's factory default setting.
Ports 1-4	Four 10/100Mbps Ethernet Port for connecting the 4 Port ADSL Router to the network devices, such as PCs.
AC Jack	12VAC/1A or 9VAC/1A Power adapter outlet.
ON/OFF	Power Switch to ON/OFF the 4 Port ADSL Router.

Press the "Reset" button will "Reboot & Restore" the ADSL Router's factory defaults and clear all the setting.

2.1.2 Front Panel

The 4 Port ADSL Router's LEDs indicators display information about the device's status.



PWR	Steady green light indicates the router is powered on.
1 : LINK/ACT	Steady green light indicates a valid Ethernet connection. Blinking green light indicates active Ethernet session.
2 : LINK/ACT	Steady green light indicates a valid Ethernet connection. Blinking green light indicates active Ethernet session.
3 : LINK/ACT	Steady green light indicates a valid Ethernet connection. Blinking green light indicates active Ethernet session.
4 : LINK/ACT	Steady green light indicates a valid Ethernet connection. Blinking green light indicates active Ethernet session.
RXD	Blinking green light indicates an active WAN session.
ADSL	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled.
RDY	4 Port ADSL Router system status indicator. When blinking indicates ADSL system is alive.

2.1.3 Connection Mechanism

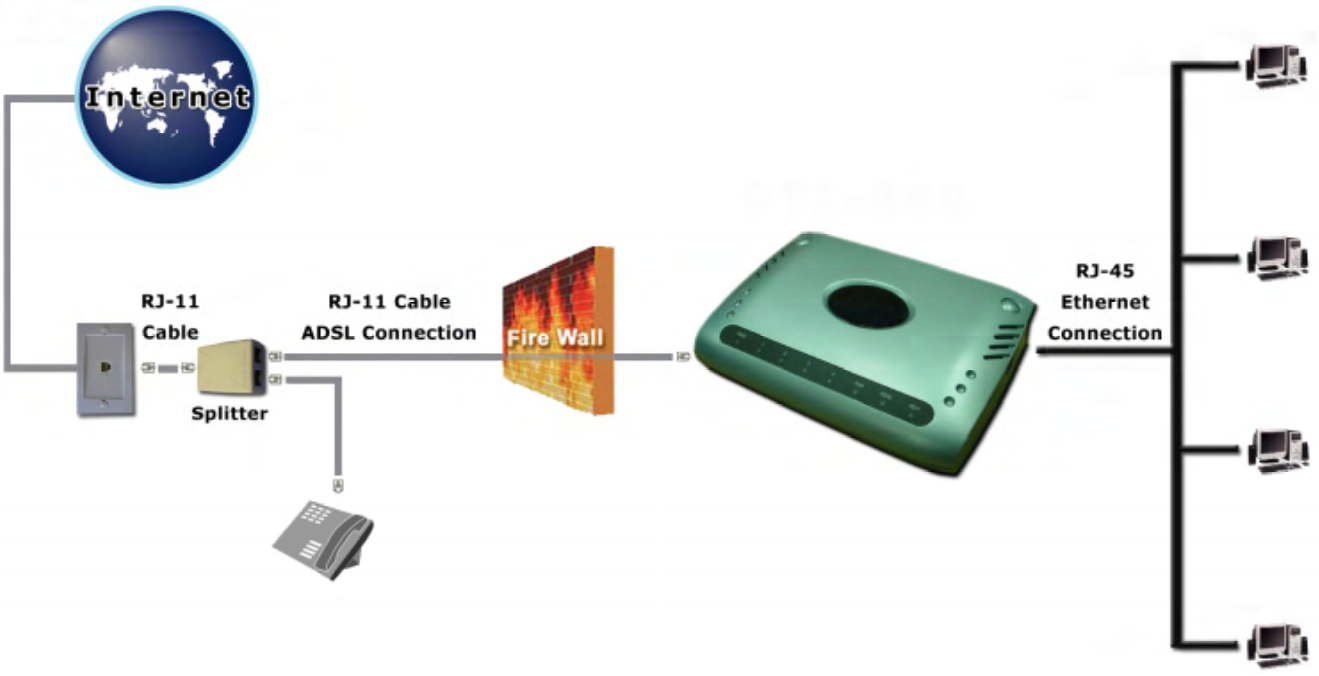
This section describes the hardware connection mechanism of your 4 Port ADSL Router on your Local Area Network (LAN) connect to the Internet, how to configure 4 Port ADSL Router for Internet access or how to manually configure your Internet connection.

You need to prepare the following items before you can establish an Internet connection through your 4 Port ADSL Router:

1. A computer which must have an installed Ethernet Adaptor and an Ethernet Cable.
2. An ADSL service account and configuration information provided by your Internet Service Provider (ISP). You will need one or more of the following configuration parameters to connect your ADSL Router to the Internet:

    a. VPI/VCI parameters
    b. Multiplexing Method
    c. Host and Domain Names
    d. ISP Login Name and Password
    e. ISP Domain Name Server (DNS) Address
    f. Fixed or Static IP Address.

Figure below shows the overall hardware connection mechanism of your 4 Port ADSL Router.



The LAN port of the 4 Port ADSL Router supports auto crossover capability.

Follow the following steps or instructions for connecting your 4 Port ADSL Router :

1. Turn off your computer.
2. Connect the ADSL port of your 4 Port ADSL Router to the splitter DSL port with a RJ-11 cable.
3. Connect the Ethernet cable (RJ-45) from your 4 Port ADSL Router to the Ethernet Adaptor in your computer.
4. Connect the Power adaptor to the 4 Port ADSL Router and plug the other end into a Power outlet.
5. Turn on your 4 Port ADSL Router.

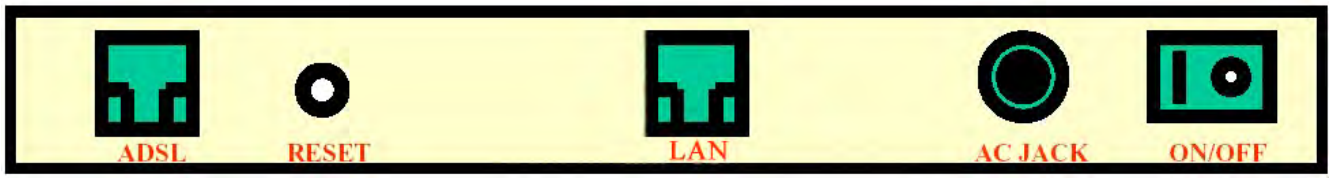
The Power light will lit after turning on the 4 Port ADSL Router.
Auto and self diagnostic process will turn the LED indicators ON and OFF during the process.

6. Turn on your computer.
7. Refer to the next chapter to setup or configure your Network Adaptor.

2.2 For One Port ADSL Router

2.2.1 Back Panel

The back panel of the 1 Port ADSL Router contains WAN/LAN Connection, USB Port Connection and Power Switch.



ADSL	Port for connecting the 1 Port ADSL Router to the ADSL Service Provider.
RESET	Restore the 1 Port ADSL Router's factory default setting.
LAN	Ethernet Port for connecting the 1 Port ADSL Router to the network devices, such as PCs.
AC Jack	12VAC/1A or 9VAC/1A Power adapter outlet.
ON/OFF	Power Switch to ON/OFF the 1 Port ADSL Router.

Press the "Reset" button will "Reboot & Restore" the ADSL Router's factory defaults and clear all the setting.

2.2.2 Front Panel

The 1 Port ADSL Router's LEDs indicators display information about the device's status.

PWR	Steady green light indicates the router is powered on.
LINK/ACT	Steady green light indicates a valid Ethernet connection. Blinking green light indicates active Ethernet session.
RXD	Blinking green light indicates an active WAN session.
ADSL	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled.
RDY	1 Port ADSL Router system status indicator. When blinking indicates ADSL system is alive.

2.2.3 Connection Mechanism

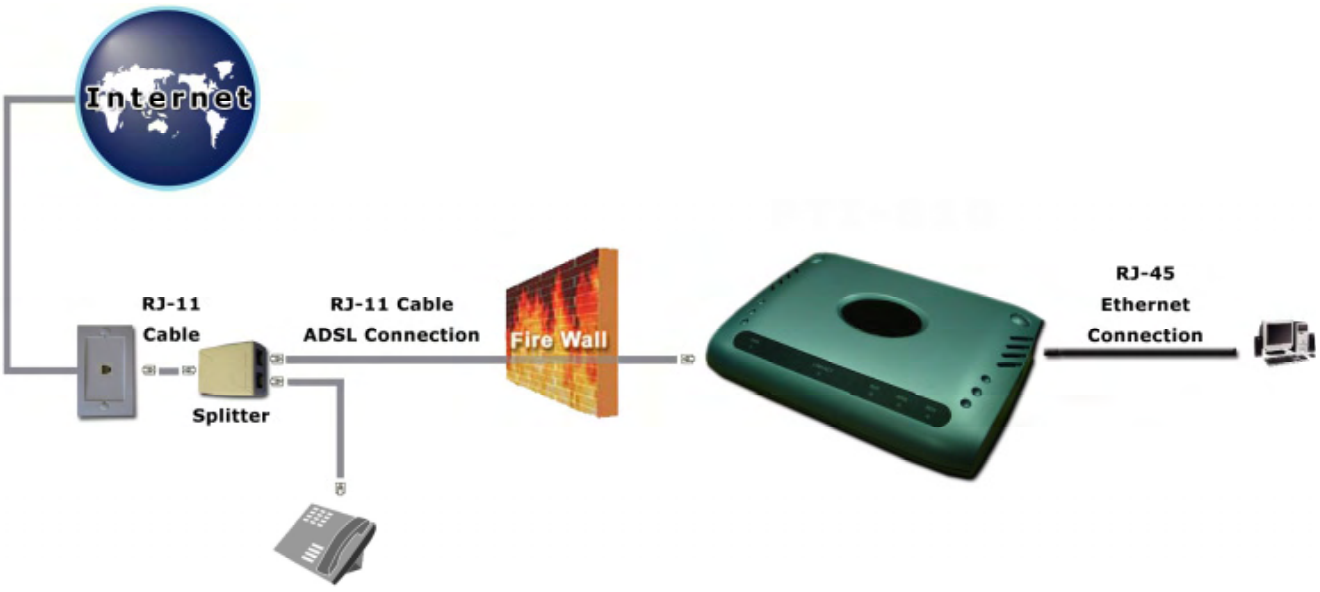
This section describes the hardware connection mechanism of your 1 Port ADSL Router on your Local Area Network (LAN) connect to the Internet, how to configure 1 Port ADSL Router for Internet access or how to manually configure your Internet connection.

You need to prepare the following items before you can establish an Internet connection through your 1 Port ADSL Router:

3. A computer which must have an installed Ethernet Adaptor and an Ethernet Cable.
4. An ADSL service account and configuration information provided by your Internet Service Provider (ISP). You will need one or more of the following configuration parameters to connect your 1 Port ADSL Router to the Internet:

    a. VPI/VCI parameters
    b. Multiplexing Method
    c. Host and Domain Names
    d. ISP Login Name and Password
    e. ISP Domain Name Server (DNS) Address
    f. Fixed or Static IP Address.

Figure below shows the overall hardware connection mechanism of your 1 Port ADSL Router.



The LAN port of the 1 Port ADSL Router supports auto crossover capability.

Follow the following steps or instructions for connecting your 1 Port ADSL Router :

8. Turn off your computer.
9. Connect the ADSL port of your 1 Port ADSL Router to the splitter DSL port with a RJ-11 cable.
10. Connect the Ethernet cable (RJ-45) from your 1 Port ADSL Router to the Ethernet Adaptor in your computer.
11. Connect the Power adaptor to the 1 Port ADSL Router and plug the other end into a Power outlet.
12. Turn on your 1 Port ADSL Router.

The Power light will lit after turning on the 1 Port ADSL Router.
Auto and self diagnostic process will turn the LED indicators ON and OFF during the process.

13. Turn on your computer.
14. Refer to the next chapter to setup or configure your Network Adaptor.

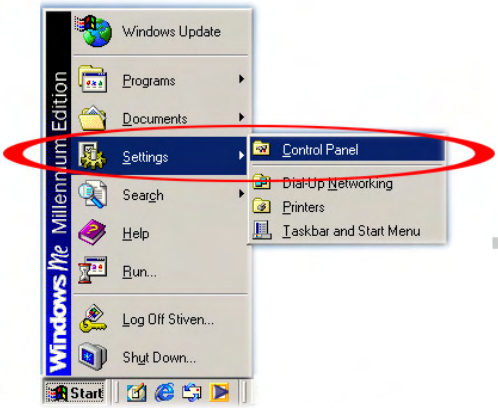
Chapter 3. Administrator's Computer Setting

The instruction in this section will help you configure your computers to be able to communicate with this ADSL Router.

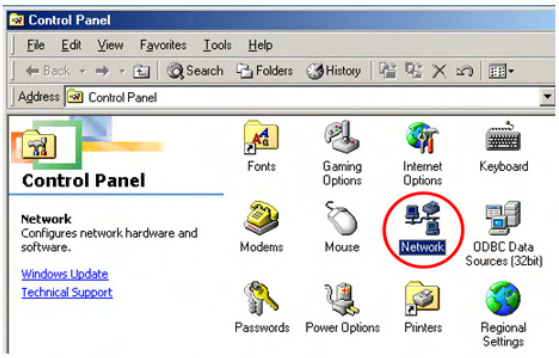
Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

The following description assumes the ADSL Router been set to factory default. (If not, please hold the reset button down for 10 seconds). The default ADSL Router's LAN IP is **10.0.0.2**.
Follow the procedures below to set your computer function as a **DHCP Client**.

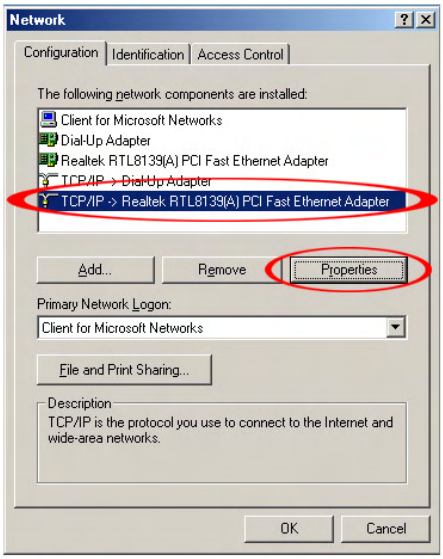
3.1 Windows 98/ME



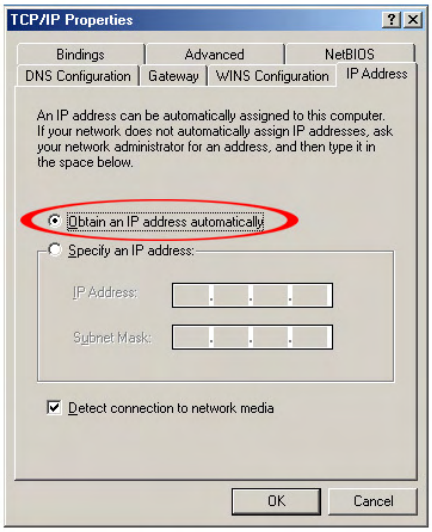
Step 1: Click Start → Setting → Control Panel.



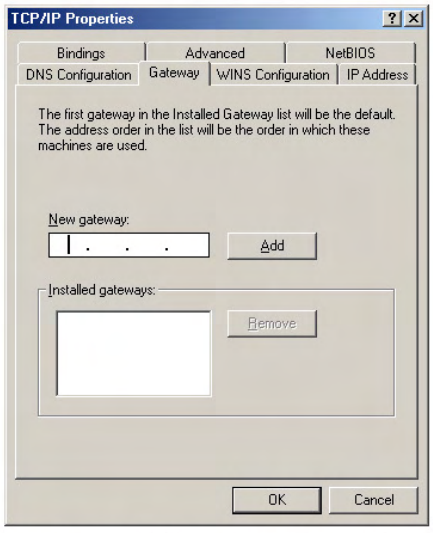
Step 2: Double-click the Network icon.



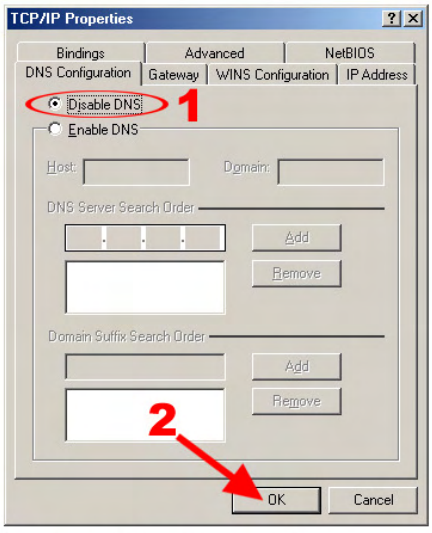
Step 3: Select the network adapter installed and click on Properties.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

Step 4: Select Obtain an IP address automatically.

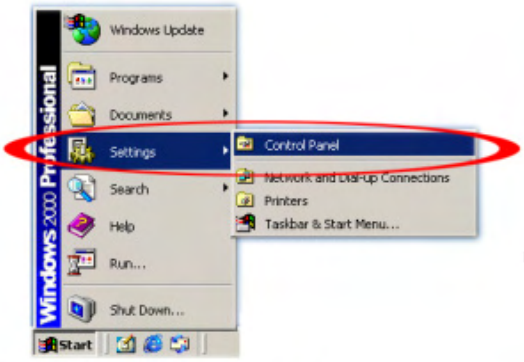


Step 5: Erase all the gateway setting.



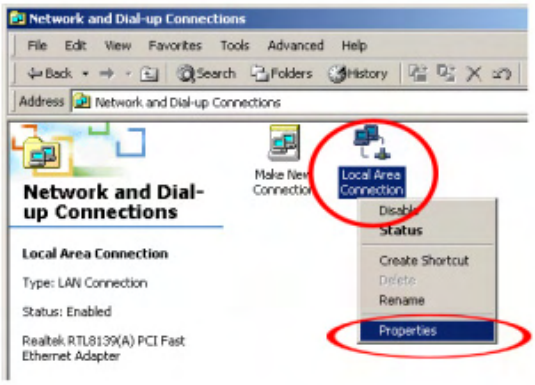
Step 6: Select Disable DNS then click OK.

3.2 Windows 2000

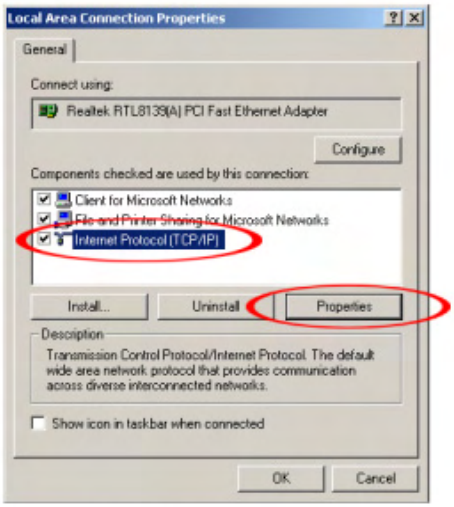


Step 1: Click Start → Setting → Control Panel.

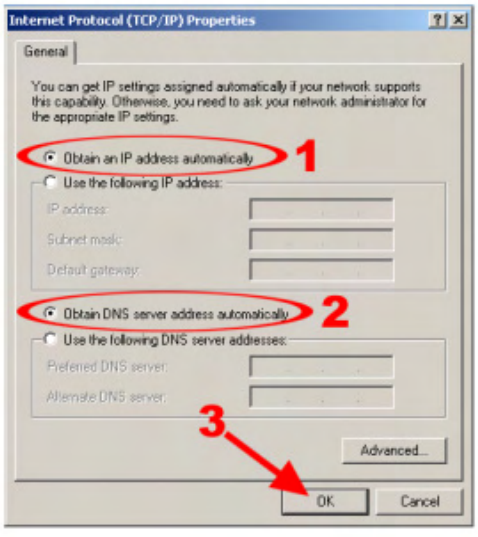
Step 2: Double-click the Network and Dial-up Connections icon.



Step 3: Right Click on the Local Area Connection and select Properties.

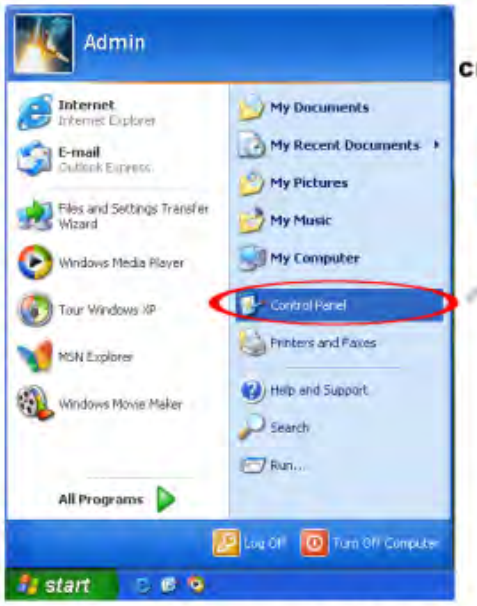


Step 4: Select Internet Protocol (TCP/IP) and click Properties.



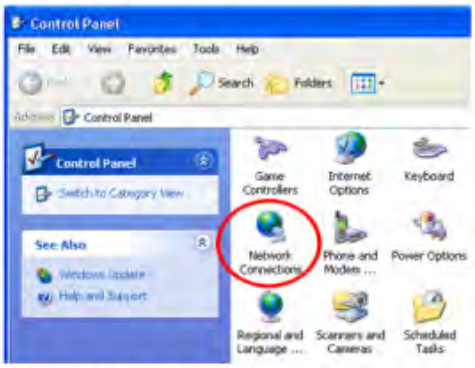
Step 5: Select Obtain and IP address automatically and NObtain DNS server address automatically. Then Click on OK.

3.3 Windows XP

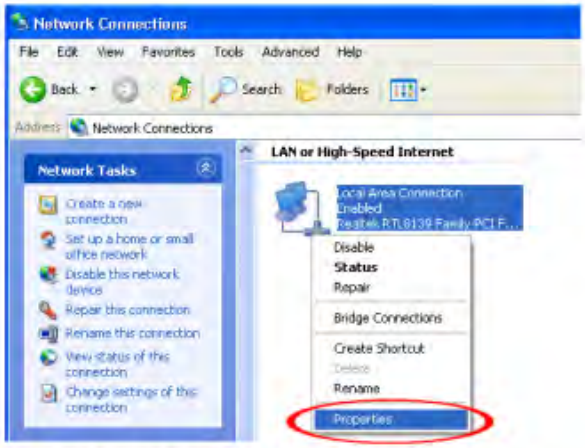


Step 1: Click **Start → Control Panel.**

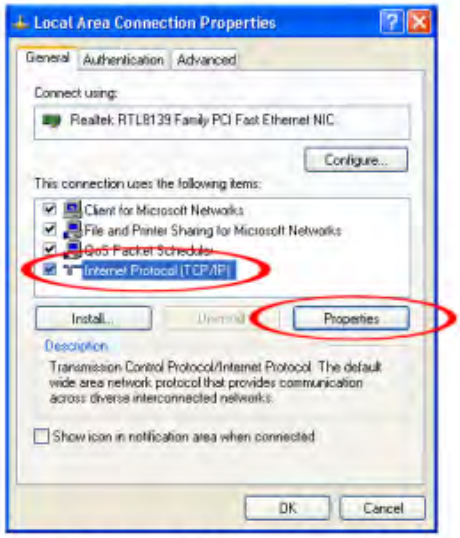
Click **Switch to Classic**



Step 2: Double-click the **Network Connections** icon.



Step 3: Right Click on the **Local Area Connection** and select **Properties.**



Step 4: Select **Internet Protocol (TCP/IP)** and click **Properties.**

Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
1
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
2
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
3
Advanced...
OK
Cancel

Step 5: Select **Obtain and IP address automatically** and **NObtain DNS server address automatically. Then Click on OK.**

Chapter 4. Device Administration

For your convenience, an Administrative Utility has been programmed into the ADSL Router. This chapter will explain all the functions in this utility. All ADSL Router based administrative tasks are performed through this web utility.

4.1 Login

Levels of Access : There are two levels of access rights/privileges for the ADSL Router:

- Administrator : User name admin, the administrator account has complete read/write access on all pages (Status, Configuration, Admin Privilege, and Firewall Configuration). Admin account also has FTP server access.
- User : User name user, the User account has read/write access to pages under the Status and Configuration sections.

The following steps will enable you to log into the ADSL Router.

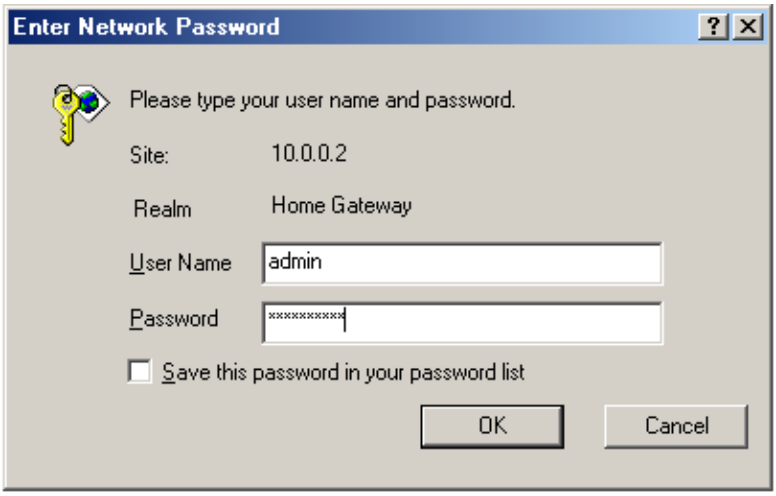
1. Launch the Web browser (Internet Explorer, Netscape, etc.).

2. Enter the LAN port default IP address (default gateway) http://10.0.0.2 in the address bar.

3. Entry of the username and password will be prompted. Enter the default login **User Name** and **Password** :

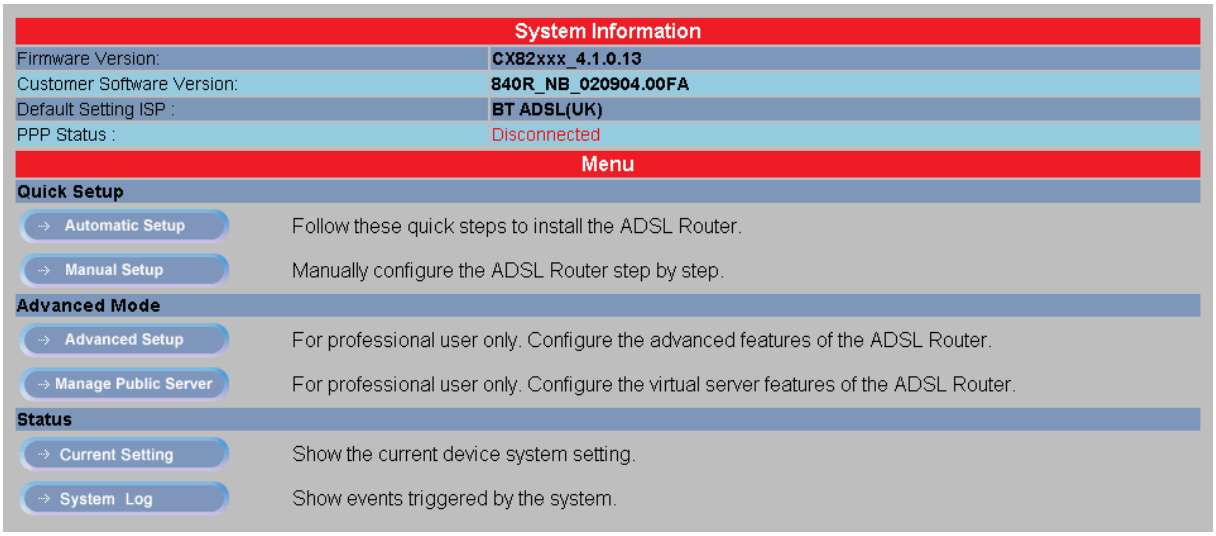
   - The default login User Name of the administrator is **"admin"**, and the default login Password is **"epicrouter"**.
   - The default login User Name for the non-administrator is **"user"**, and the default login Password is **"password"**.

4. **Remember my password** check box : By default, this box is not checked. Users can check this box so that Internet Explorer will remember the User name and Password for future logins. It is recommended to leave this box unchecked for security purposes.



"Admin" and **"User"** passwords can be changed after login. Refer to Section 4.3.2.8 for User Password configuration and Section 4.3.3.9 for Admin Password configuration for further instruction.

Upon entering the address into the web browser, the configurable main page with all the device status information will pop up as shown in Figure below :



1. **System Information** : Show the current ADSL Router Firmware version, Customer Software version, Current ISP setting and PPP Status

2. **Menu** : Describe the way to Setup/Configuration your ADSL Router.

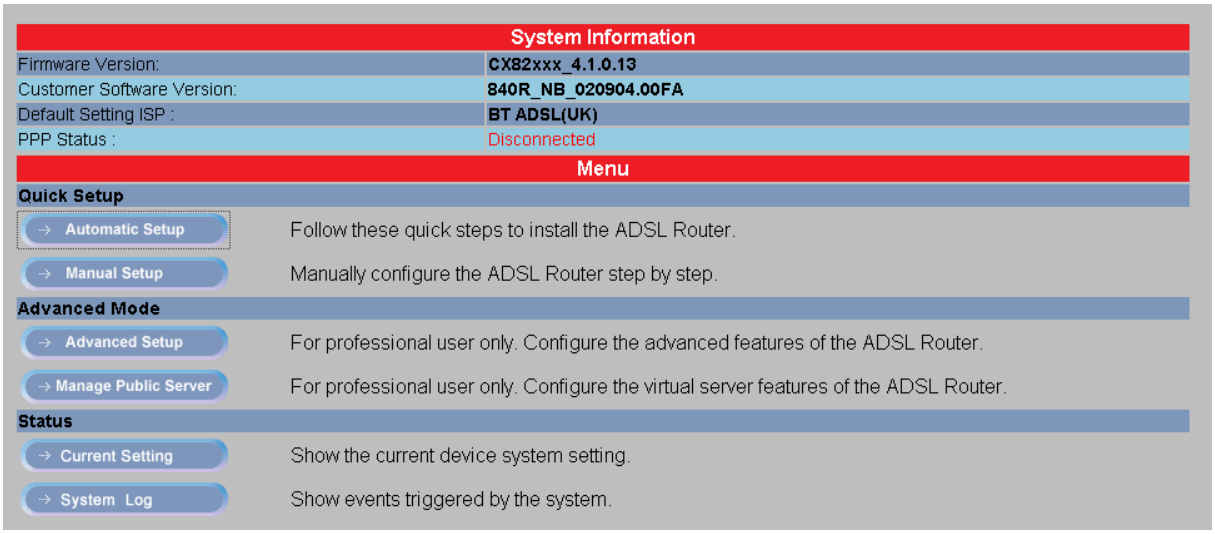
   A. **Quick Setup** : The Quick Setup is meant to help you install the ADSL Router Quickly and easily.
      i. **Automatic Setup** : Automatic Setup by selecting country and ISP from the list step by step.
      ii. **Manual Setup** : Entering all the setting/configuration manually. Check your ISP for the setting details.

   B. **Advanced Mode** : The Advanced Mode describe the detail instruction on installation /configurations for advance user. No changes should be made to this section without a thorough understanding of networking concepts.
      i. **Advanced Setup** : For professional user ONLY. No changes should be made to this section without a thorough understanding of networking concepts.
      ii. **Manage Public Server** : For professional user ONLY. No changes should be made to this section without a thorough understanding of networking concepts.

   C. **Status** : Display the ADSL Router's current or previous connection, setting and configuration status. All the information provided under the Status tab are read only and can be changed upon setting/configuration of the ADSL Router.
      i. **Current Setting** : Shows the current setting/configuration status.
      ii. **System Log** : Shows the System connection information.

4.2 Quick Setup

The Quick Setup is meant to help you install the ADSL Router quickly and easily. Click “Automatic Setup” and follow the steps describe below to complete your installation.

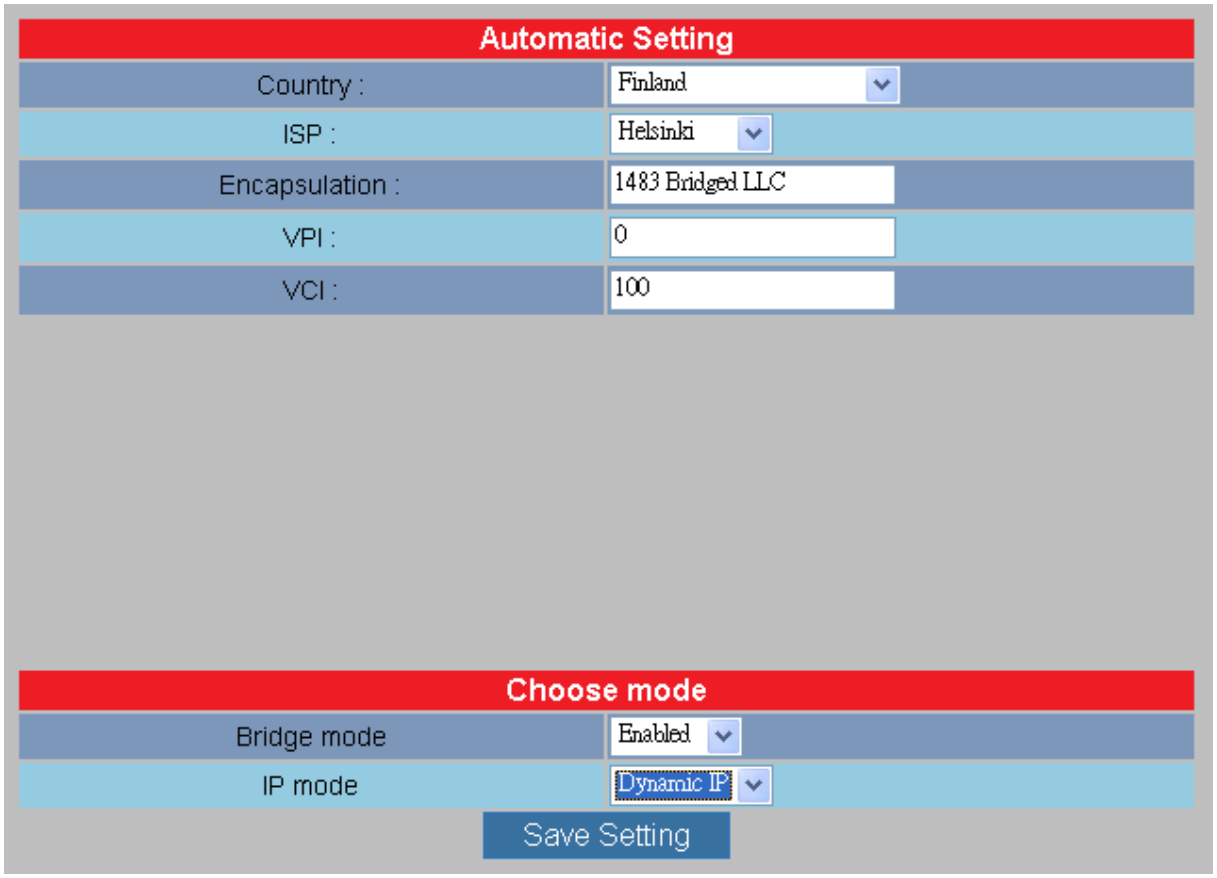


4.2.1 Quick Setup : Automatic Setting

STEP 1. Select the presetting country form the list.

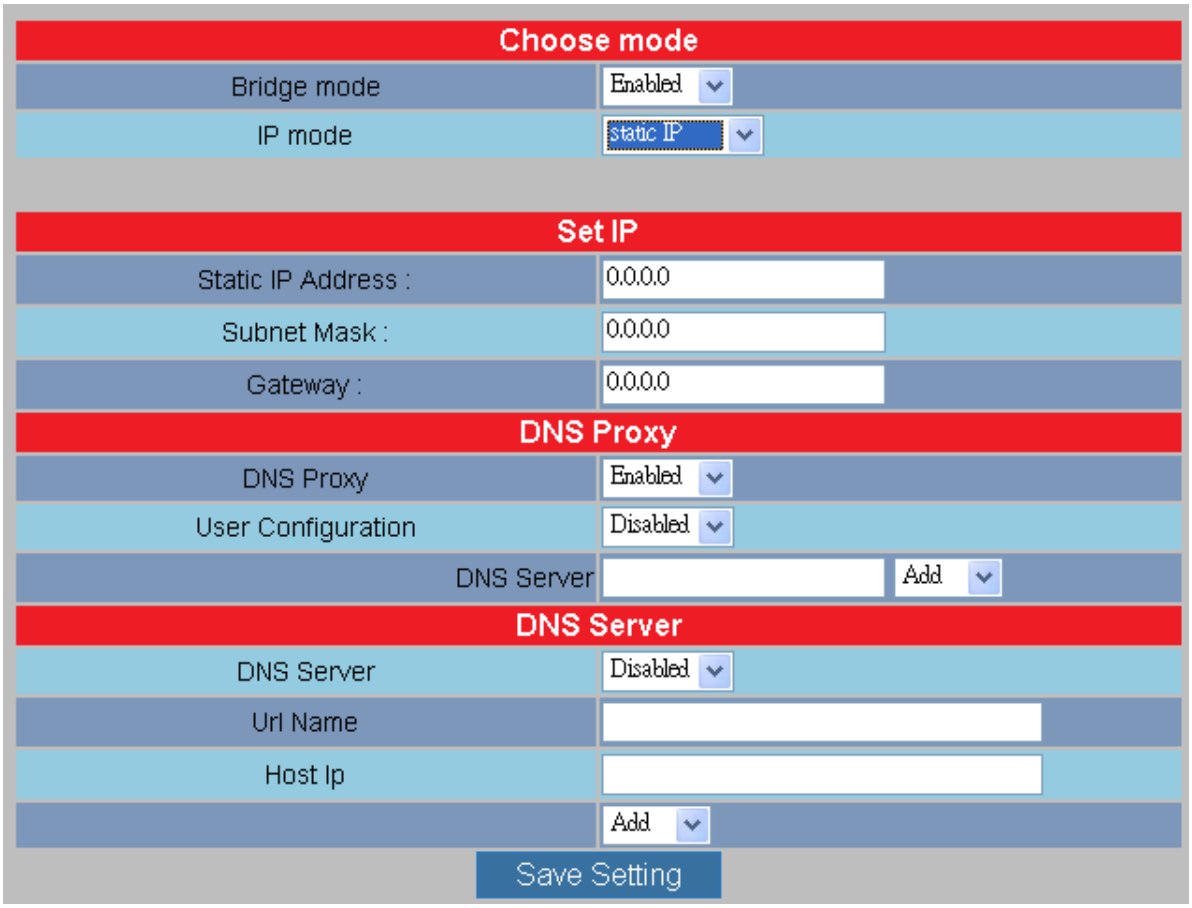
- For 1483 Bridged LLC encapsulation, there are two available IP mode :

  i. Bridge Mode : Click “Enable” or “Disable” for the connection mode. Check your ISP for the connection/setting details.



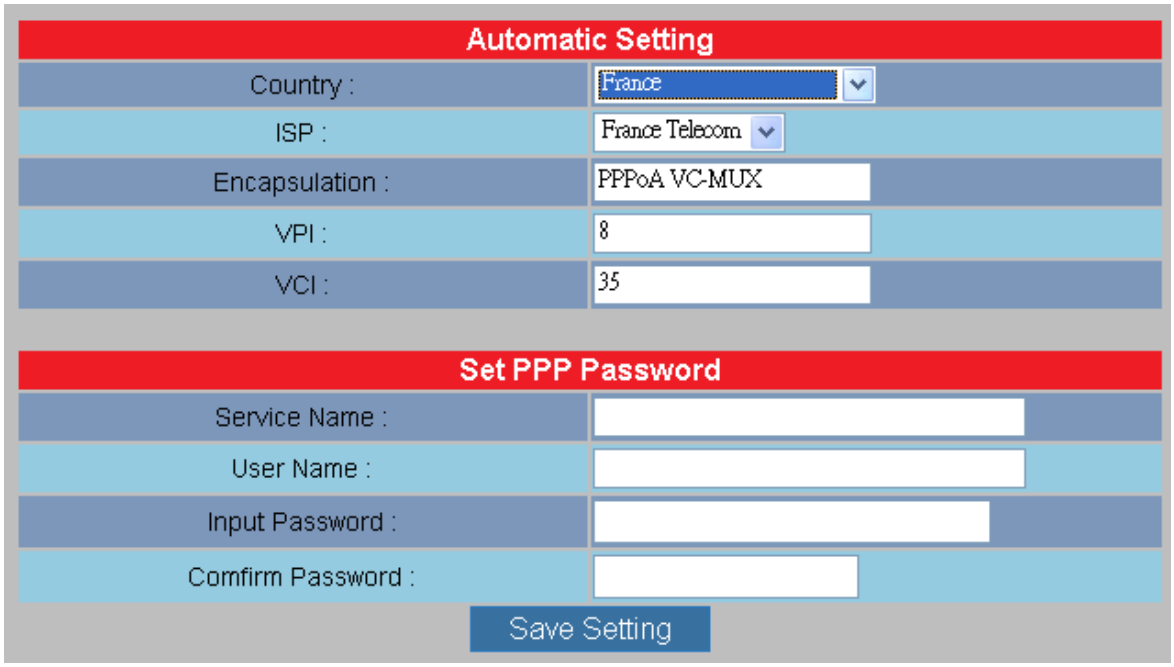
  ii. IP Mode : Click “Dynamic IP” or “Static IP” for the connection mode. Check your ISP for the connection/setting details.

  If “Static IP” mode is chosen, more terms need to be filled before any Internet access is available. Check your ISP for the setting/configuration details.



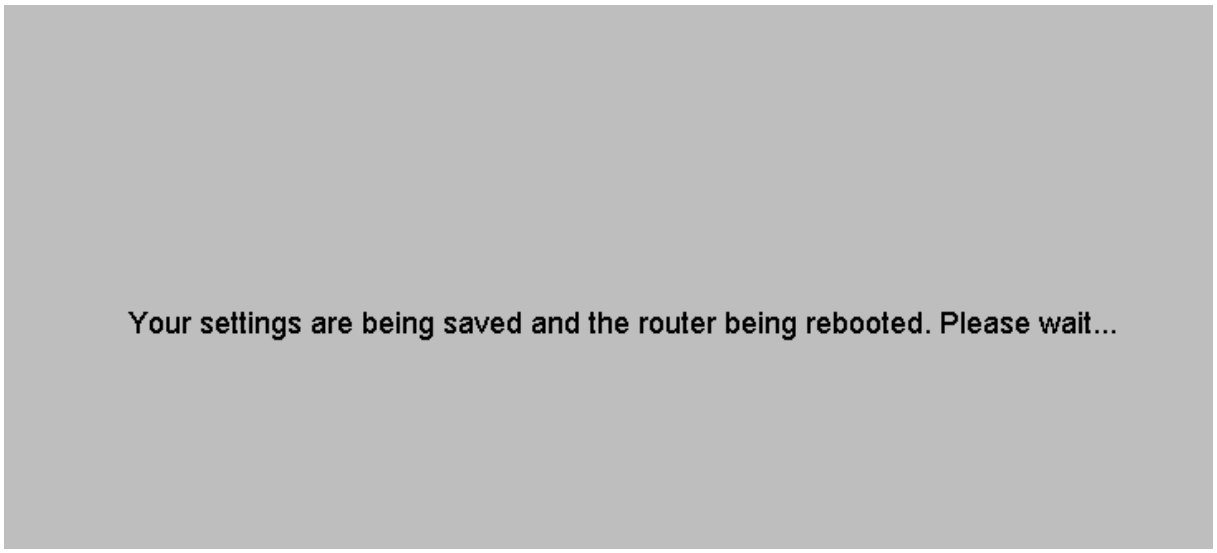
◆ For PPPoA VC-Mux and PPPoE LLC encapsulation :

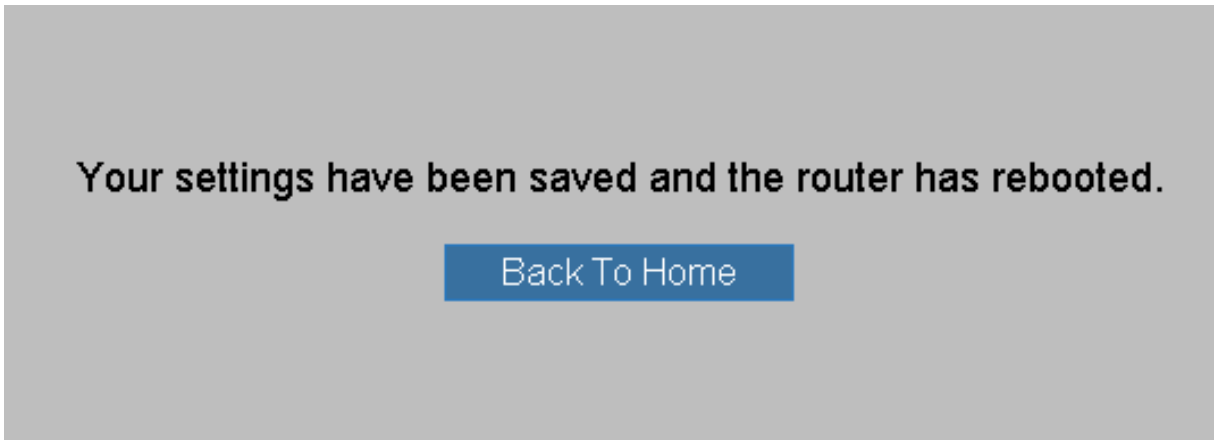
Manually enter your “Service Name”, “User Name” and “Password” which will be provided by your ISP. Check your ISP for the details.



STEP 2. Click “Save Setting” after your choice.

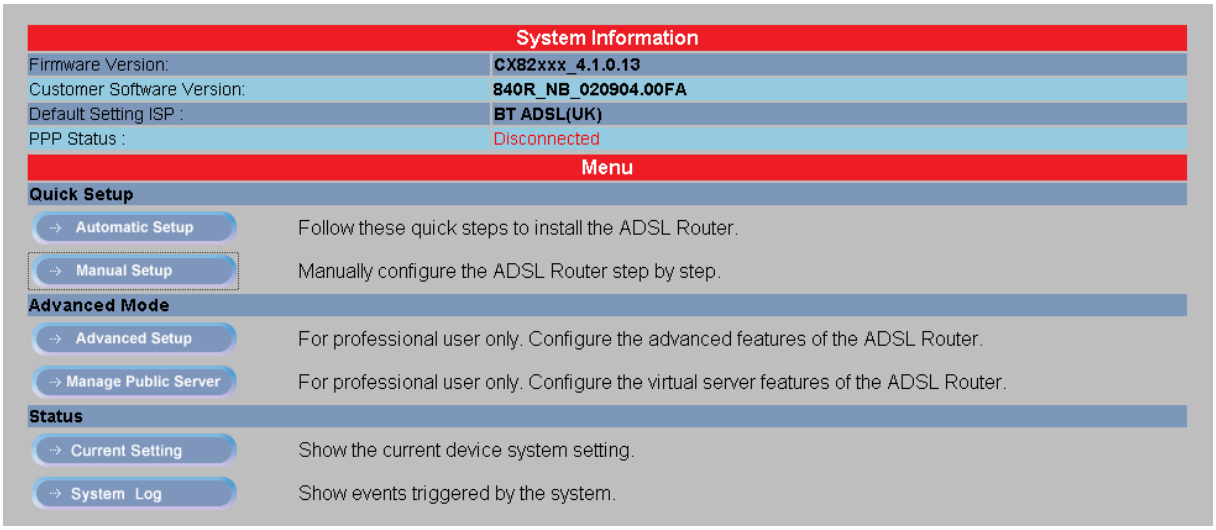
The ADSL Router system will reboot and activate your setting. Click “**Back To Home”** after the reboot process. Connection to the Internet is available after the above process.



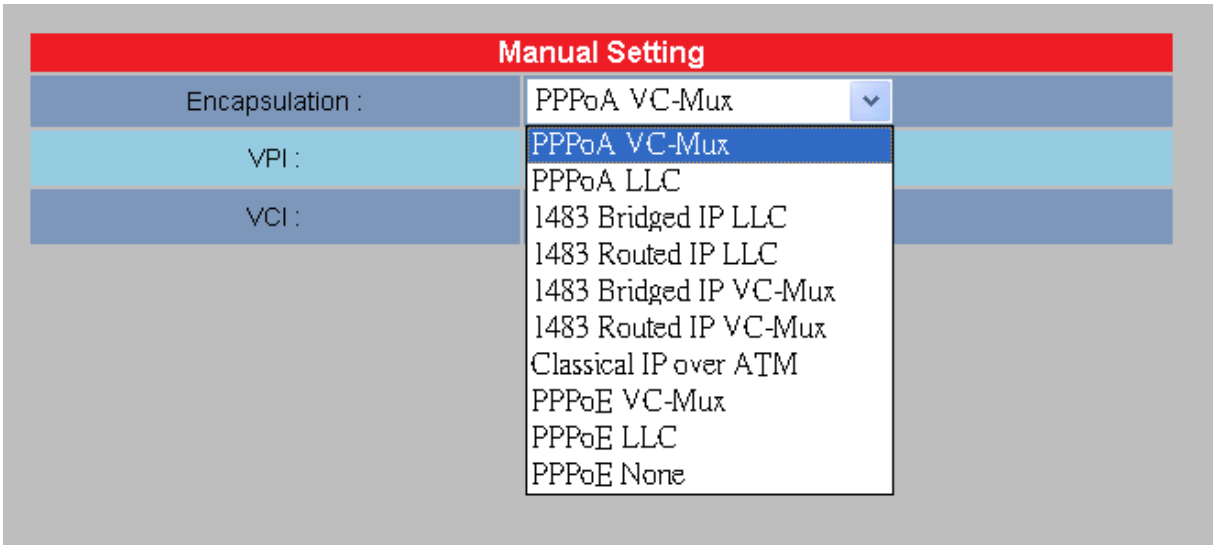


4.2.2 Quick Setup : Manual Setup

"Manual Setup" allows you to manually configure the ADSL Router step by step by selecting User Configured in the field. Click **"Manual Setup"** and follow the installation wizard to complete the installation process.



Manually enter the **"Encapsulation"** type, **"VPI"** and **"VCI"** setting. Check your ISP for the setting/configuration details. These modes are guidelines for setting up the WAN interface. Table below lists the example of the mode configurations.



WAN Configuration	Bridge Mode	Router Mode (PPPoA/PPPoE)	Router Mode (Dynamic IP)	Router Mode (Static IP)	Half Bridge
IP address	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP	Automatically assigned by ISP
Subnet Mask	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP	Automatically assigned by ISP
Gateway	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP	Automatically assigned by ISP
Encapsulation	1483 Bridged IP LLC, 1483 Bridged IP VC-Mux	PPPoA LLC/ VC-Mux, PPPoE LLC/ VC-Mux	1483 Bridged/ Routed IP LLC, 1483 Bridged/ Routed VC-Mux, Classical IP over ATM	1483 Bridged/ Routed IP LLC, 1483 Bridged/ Routed VC-Mux, Classical IP over ATM	PPPoA LLC/ VC-Mux, PPPoE LLC/ VC-Mux
Bridge	Enabled	Disabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A	Provided by ISP
PPP User name	N/A	Provided by ISP	N/A	N/A	Provided by ISP
PPP Password	N/A	Provided by ISP	N/A	N/A	Provided by ISP
DHCP Client enable	Unchecked	Unchecked	Checked	Unchecked	Unchecked
PPP Half Bridge	Disabled	Disabled	Disabled	Disabled	Enabled (automatically configured the DHCP Server, NAT, and DNS Proxy)
DHCP Server	Disabled	Enabled	Enabled	Enabled	Enabled
NAT	Disabled	Enabled (Dynamic NAPT)	Enabled (Dynamic NAPT)	Enabled (Dynamic NAPT)	Disabled
DNS Proxy	Disabled	Enabled	Enabled	Enabled	Disabled

A. **Bridge Mode:** Bridge Mode is used when there is one PC connected to the LAN-side Ethernet port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet) side, i.e., to store and forward. There are two encapsulation type for Bridge Mode :

i. **1483 Bridged IP LLC** : If 1483 Bridged IP LLC mode is selected, select **"Enable"** or **"Disable"** to activate the WAN configuration setting. Select **"Dynamic IP"**, which will automatically assigned by your ISP or **"Static IP"**, which will be provided by your ISP.

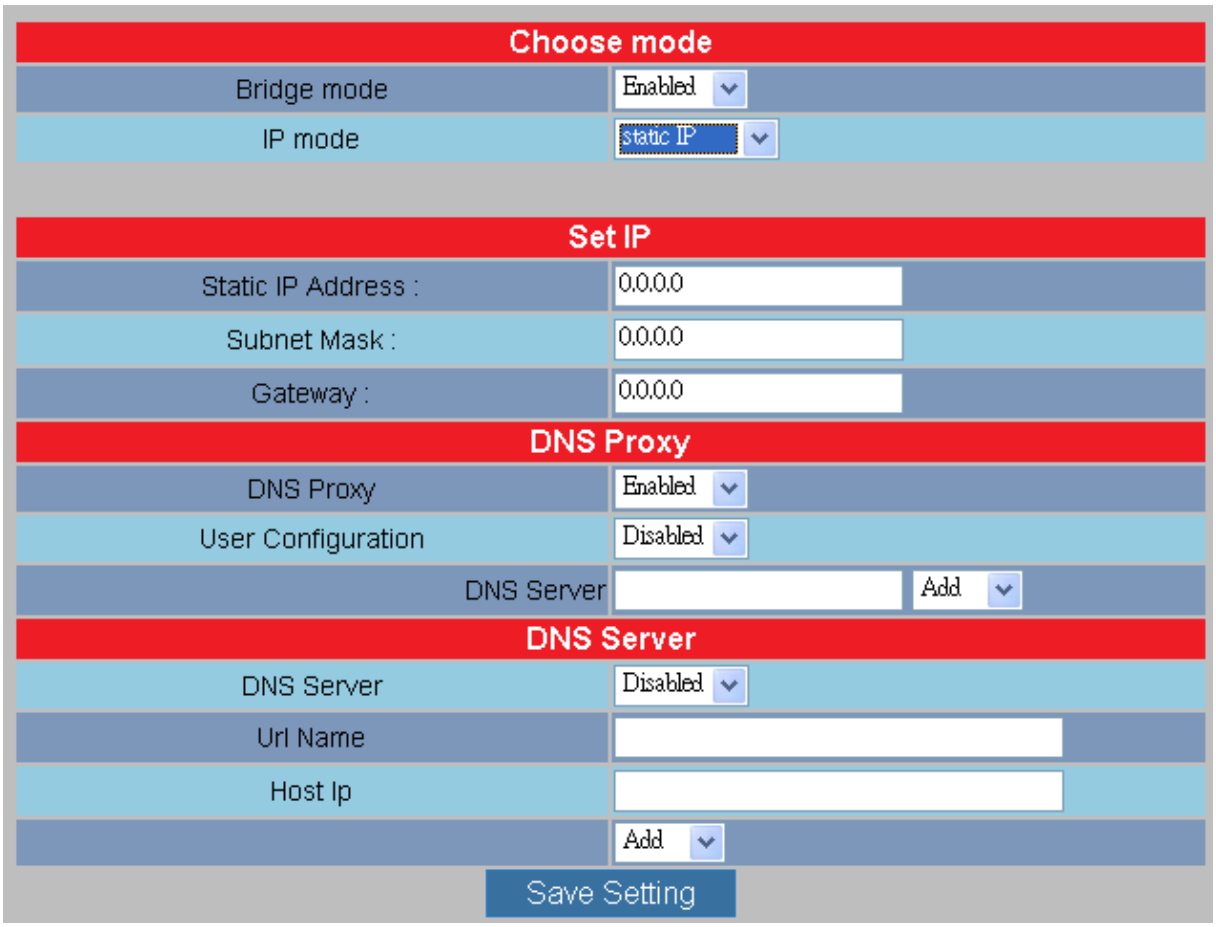
ii. **1483 Bridged IP VC-Mux** : If 1483 Bridged IP VC-Mux mode is selected, select **"Enable"** or **"Disable"** to activate the WAN configuration setting. Select **"Dynamic IP"**, which will automatically assigned by your ISP or **"Static IP"**, which will be provided by your ISP.

iii. **1483 Routed IP LLC** : If 1483 Router IP LLC mode is selected, select **"Enable"** or **"Disable"** to activate the WAN configuration setting. Select **"Dynamic IP"**, which will automatically assigned by your ISP or **"Static IP"**, which will be provided by your ISP.

iv. **1483 Routed IP VC-Mux** : If 1483 Routed IP VC-Mux mode is selected, select **"Enable"** or **"Disable"** to activate the WAN configuration setting. Select **"Dynamic IP"**, which will automatically assigned by your ISP or **"Static IP"**, which will be provided by your ISP.

For **"Dynamic IP"**, nothing have to fill in, just click **"Save Setting"** to activate your configuration.

For **"Static IP"**, please check with your ISP to fill in the necessary setting before clicking **" Save Setting"** to activate your configuration.



- **"Set IP"** : Static IP Settings are for users who have a Static IP Address (WAN side) from their ISP.

  ☑ **"Static IP Address" :** This is the static IP Address given by the ISP. *Range for IP Address is x.x.x.y, where 0 ≦ x≦ 255 and 1 ≦ y≦ 254, default is 192.168.241.101.*

  ☑ **"Subnet Mask" :** This is the subnet mask given by the ISP.

  Range for Subnet Mask is x.x.x.x, where 0 ≦ x ≦ 255, default is 255.255.255.0

  ☑ **"Gateway" :** This is the Gateway given by the ISP.

  Range for Gateway is x.x.x.y, where 0 ≦ x≦ 255 and 1 ≦ y≦ 254, default is 0.0.0.0.

- **"DNS Proxy"** : The DNS proxy on the ADSL Router records the available DNS servers and forwards DNS query messages to one of DNS servers.

  - ☑ **"DNS Proxy Enable/Disable" :** When the DNS Proxy is Disabled, the LAN port does not process the DNS query message. For the DHCP requests from local PCs, the DHCP server will set the user-configured DNS server as the DNS server. Then all DNS query messages will be directly sent to the DNS servers. DNS Proxy is enabled by default.

  - ☑ **"Auto Discovered Enable/Disable" :** When enabled (default), the DNS proxy will store the DNS server IP addresses obtained from DHCP client or PPP into the table. All DNS query messages will be sent to the dynamically obtained DNS server. Select this option when the DNS Server address is unknown but provided (automatically) by the ISP.

  - ☑ **"User Configured Enable/Disable" :** When enabled, the DNS proxy will use the user-configured DNS server. All DNS query messages will be sent to the DNS server. Enter the DNS IP in the DNS Server field. Select this option when the DNS Server address assigned by the ISP is known. User Configured is disabled by default.

- **"DNS Server"** : This is the user defined DNS server URL name and IP. Default is **"Disable"**.

  - ☑ **"URL Name Add/Delete"** : This is the URL name for the DNS server. This can be up to 255 characters.

  - ☑ **"Host IP (Add Only)"** : This is the IP address of the DNS Server.

- **"Save Setting"** : Clicking this will link the user to the **"Save Settings"** page.

B. **Router Mode :** Router Mode is used when there is more than one PC connected to the LAN-side Ethernet port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address. There are four encapsulation type for Router Mode :

   i. **PPPoA VC-Mux** : If PPPoA VC-Mux mode is selected, manually enter your **"User Name"**, **"Input Password"** and **"Confirm Password"** then click **"Save Setting"** after your configuration. Check with your ISP for the **VPI/VCI** setting details.

   ii. **PPPoA LLC** : If PPPoA LLC mode is selected, manually enter your **"User Name"**, **"Input Password"** and **"Confirm Password"** then click **"Save Setting"** after your configuration. Check with your ISP for the **VPI/VCI** setting details.

iii. **PPPoE VC-Mux** : If PPPoE VC-Mux mode is selected, manually enter your **"User Name"**, **"Input Password"** and **"Confirm Password"** then click **"Save Setting"** after your configuration. Check with your ISP for the **VPI/VCI** setting details.

iv. **PPPoE LLC** : If PPPoE LLC mode is selected, manually enter your **"User Name"**, **"Input Password"** and **"Confirm Password"** then click **"Save Setting"** after your configuration. Check with your ISP for the **VPI/VCI** setting details.

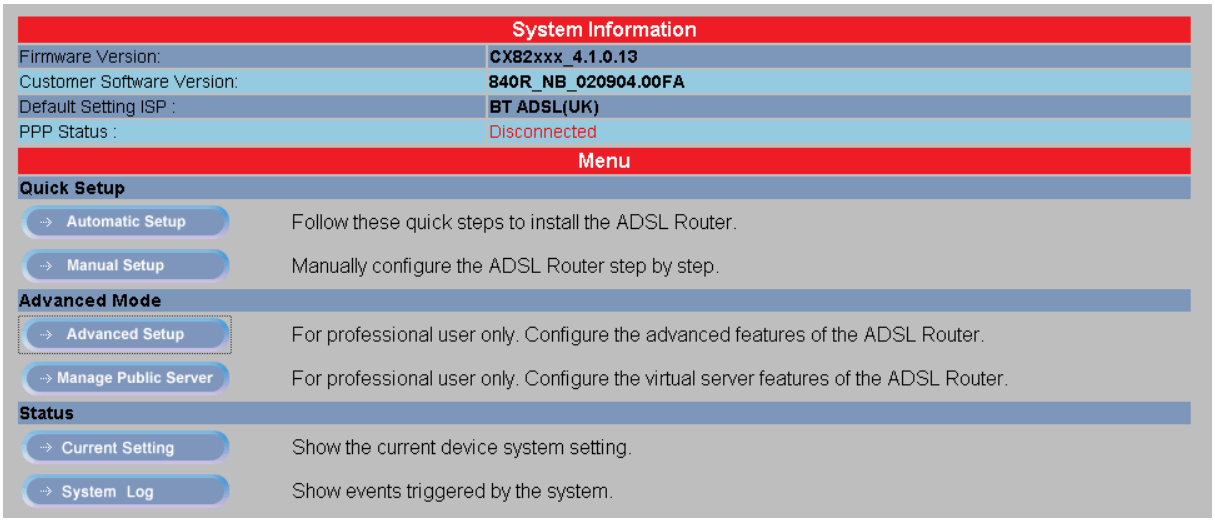
- **PPP Half Bridge:** Although the Router mode is capable of terminating the PPP in the modem and hence does not require PPPoE client software on the host PC, there are some disadvantages to Router mode when only single-user support is required. For instance, Router mode uses NAT which requires ALG support. PPP Half Bridge also terminates the PPP in the modem and does not require a PPPoE client on the PC. However, PPP Half Bridge does not use NAT and is not limited by ALGs. PPP Half Bridge will work with Ethernet interface to the PC.

- **Single-User Mode:** Only one computer is connected at the LAN side through Ethernet.

- **Multi-User Mode:** Multiple computers are connected at the LAN side through Ethernet.

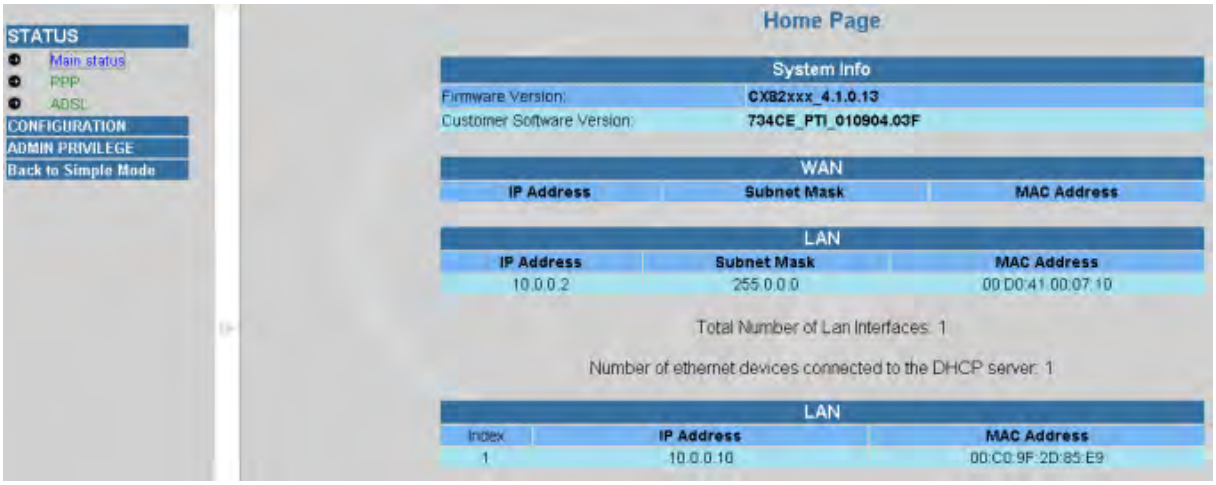
4.3 Advanced Mode

The Advanced Mode describe the detail instruction on installation/configurations for advance user. Click **"Advanced Setup"** icon to login the configuration/setting pages.



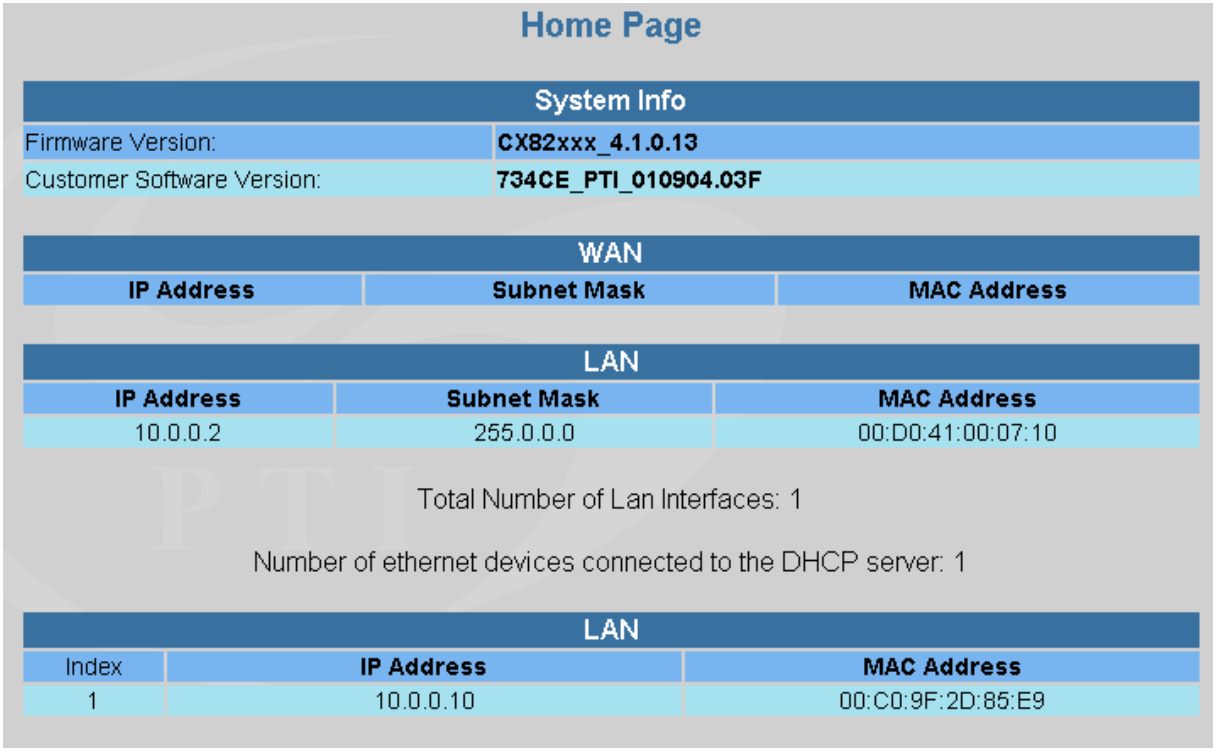
4.3.1 Advanced Setup—Status

Click **"Advanced Setup"**, the device **"Home Page"** or **"Main Status"** window will pop up. It shows all the current setting/configuration information of the ADSL Router.



4.3.1.1 Status – Main Status

The links under the **Main Status** column are associated with the pages that represent the status of system (computer and ADSL Router) and interfaces (Connections). This includes LAN, WAN and ADSL status. These pages can be viewed and modified by both **user** and **admin** accounts.



Home Page

System Info	
Firmware Version:	**CX82xxx_4.1.0.13**
Customer Software Version:	**734CE_PTI_010904.03F**

WAN		
IP Address	**Subnet Mask**	**MAC Address**

LAN		
IP Address	**Subnet Mask**	**MAC Address**
10.0.0.2	255.0.0.0	00:D0:41:00:07:10

Total Number of Lan Interfaces: 1

Number of ethernet devices connected to the DHCP server: 1

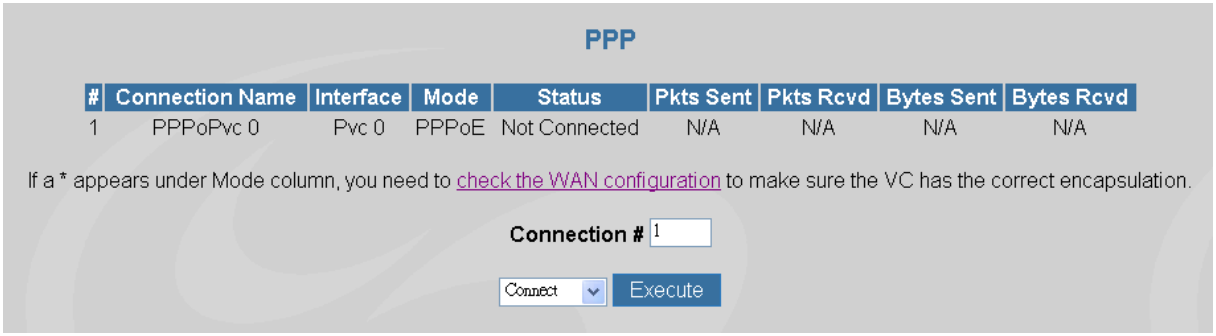
LAN		
Index	**IP Address**	**MAC Address**
1	10.0.0.10	00:C0:9F:2D:85:E9

System Info	
Firmware Version	Shows the firmware version you are using.
Customer Software Version	Shows the software control code from.
WAN	
IP Address	Shows the ADSL Router's IP Address. The default value is 10.0.0.2.
Subnet Mask	Shows the Subnet Mask of the WAN (ADSL) Interface
MAC Address	Shows the WAN MAC Address of the WAN (ADSL) Interface.
LAN	
IP Address	Shows the ADSL Router's IP Address. The default value is 10.0.0.2.
Subnet Mask	Shows the Subnet Mask of the LAN Interface
MAC Address	Shows the WAN MAC Address of the LAN Interface.
LAN	
Index	Shows the number of Ethernet device connected to the ADSL Router.
IP Address	Shows the ADSL Router's IP Address. The default value is 10.0.0.2.
MAC Address	Shows the WAN MAC Address of the LAN Interface.

4.3.1.2 Status – PPP

The **PPP Status** page shows the status of each PPP session for each PPP interface. This page contains information that is dynamic and will refresh every 8 seconds.

Note: PPP interfaces can be created, modified, and deleted in the PPP Configuration page.


PPP
Connection Name Interface Mode Status Pkts Sent Pkts Rcvd Bytes Sent Bytes Rcvd
1 PPPoPvc 0 Pvc 0 PPPoE Not Connected N/A N/A N/A N/A
If a * appears under Mode column, you need to check the WAN configuration to make sure the VC has the correct encapsulation.
Connection # 1
Connect
Execute

PPP (Point-to-Point Protocol): The table displays the following fields:

- Connection Name: This is user defined. User defined connections for PPP can be created in PPP Configuration page.
- Interface: States the interface that is being used (PVC0 ... PVC7).
- Mode: There are two available modes for the connection:
  - PPP over Ethernet (PPPoE)
  - PPP over ATM (PPPoA)
- Status: States whether PPP connection is Connected or Not Connected.
- Packets Sent: Number of packets sent by a particular PPP Connection.
- Packets Received: Number of packets received by a particular PPP Connection.
- Bytes Sent: Number of bytes sent by a particular PPP Connection.
- Bytes Received: Number bytes received by a particular PPP Connection.
- Connect and Disconnect: This field allows you to manually connect/disconnect the PPP connection for each PPP interface. In other words, each PPP session can be connected and disconnected individually.
- Connection #: Specifies the PPP session to be connected/disconnected.
- Connect/Disconnect Execute: Press this button to either connect or disconnect. Connection status dialog will be displayed below the Execute button after it is pressed. Sample dialog with explanation:

- **PPP X: Connecting...** This is displayed while the PPP session is attempting to connect to the ISP.

- **PPP X: Connect ERROR** This is displayed when a connection cannot be made due to an error.

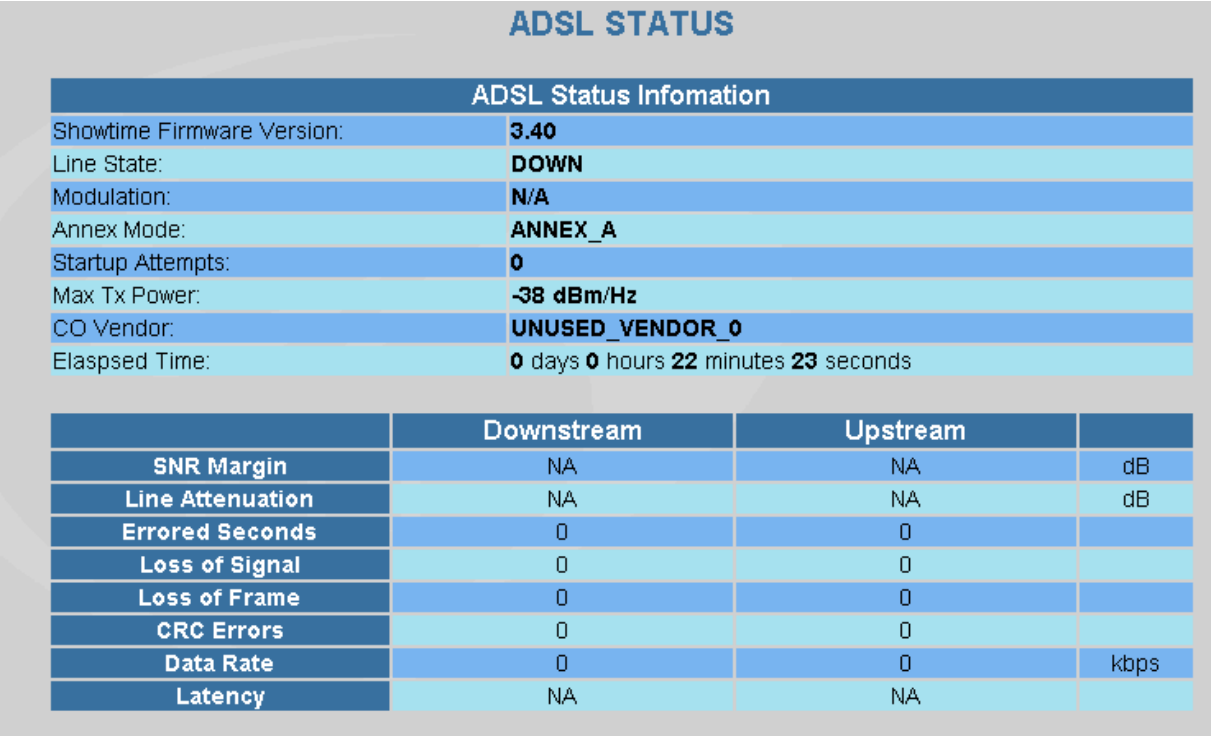
- **PPP X: is currently not connected** This is displayed when a disconnect attempt is made on a session that is not currently connected.

- **PPP X: does not exist!** This is displayed when a connect or disconnect attempt is made on a session number that does not exist.

Click **"Check the WAN configuration"** will show you all the detail WAN setting/configuration of this ADSL Router. Refer to Section 4.3.2 for details.

4.3.1.3 Status – ADSL

The **ADSL Status** page shows the ADSL physical layer or link status. The information displayed on this page is either inherent to the ADSL Router or set by the ADSL Central Office (CO) DSLAM, neither of which cannot be changed by the user. This page contains information that is dynamic and will refresh every 2 seconds.



ADSL STATUS

ADSL Status Infomation	
Showtime Firmware Version:	**3.40**
Line State:	**DOWN**
Modulation:	**N/A**
Annex Mode:	**ANNEX_A**
Startup Attempts:	**0**
Max Tx Power:	**-38 dBm/Hz**
CO Vendor:	**UNUSED_VENDOR_0**
Elaspsed Time:	**0** days **0** hours **22** minutes **23** seconds

	Downstream	Upstream	
SNR Margin	NA	NA	dB
Line Attenuation	NA	NA	dB
Errored Seconds	0	0	
Loss of Signal	0	0	
Loss of Frame	0	0	
CRC Errors	0	0	
Data Rate	0	0	kbps
Latency	NA	NA	

- Showtime Firmware Version: This field displays the ADSL data pump firmware version number.
- Line State: This field displays the ADSL connection process and status. The different states for this field are as follows:
  - Activation: The ADSL Router is in this state when it is attempting to start the activation process.
  - Initialization: The ADSL Router is initializing handshake with the CO.
  - Training: This is a part of the handshake process with the CO.
  - Channel Analysis: This is a part of the handshake process with the CO.
  - Exchange: This is a part of the handshake process with the CO.
  - Down: This indicates that the ADSL connection is down.
  - Showtime: This indicates that a connection has been established between the ADSL Router and the CO.
- Modulation: This field displays the ADSL modulation status, which can either be G.dmt or T1.413.
- Annex Mode: This field displays the ADSL annex mode, which can either be Annex A or Annex B.

- Startup Attempts: This field displays the number of ADSL connection attempts after loss of showtime. A connection attempt is recorded only if showtime is attained.

- Max TX Power: This field displays the transmit output power level of the CPE (Customer Premise Equipment), which is the transmit output power level of the ADSL Router.

- CO Vendor: This field displays the Central Office (CO) DSLAM vendor name, if available. If the ADSL Router is not connected to an ADSL vendor, then "UNUSED_VENDOR_0" will appear in this field.

- Elapsed Time: This field displays the time of the ADSL Router has been in operation.

  This is the amount of time the ADSL Router is on, not the amount of time it is connected to the PC or in ADSL status.

- SNR Margin: Signal to Noise Ratio (SNR) is the measure of signal intensity relative to the background noise. The SNR Margin is the amount of increased noise that can be tolerated while maintaining the designated BER (bit error rate). The SNR Margin is set by Central Office DSLAM. If the SNR Margin is increased, bit error rate performance will improve, but the data rate will decrease. Conversely, if the SNR Margin is decreased, bit error rate performance will decrease, but the data rate will increase.

- Line Attenuation: Attenuation is the decrease in magnitude of the ADSL line signal between the transmitter (Central Office DSLAM) and the receiver (Client ADSL Router), measured in dB. It is measured by calculating the difference in dB between the signal power level received at the Client ADSL Router and the reference signal power level transmitted from the Central Office DSLAM.

- Errored Seconds: During Showtime, if any given second contains a CRC error, then that second will be declared and recorded as an Errored Second.

- Loss of Signal: Loss of signal refers to the ADSL Router losing an ADSL signal, not the computer losing a signal with the modem. Loss of Signal event is only recorded if the signal is lost while the ADSL Router is in showtime status. This field displays the count of ADSL signal loss events.

- Loss of Frame: A frame is a unit of data in ATM. This field displays the count of ADSL frame loss events. A Loss of Frame event is only recorded if the signal is lost while the ADSL Router is in showtime status.

- CRC Errors: Cyclic Redundancy Check (CRC) is a method for checking errors in data transmissions. This field displays the number of transmit data frames containing CRC errors.

- Data Rate: This field displays the ADSL data rate in kbps.

- Latency: Latency, synonymously delay, is the amount of time it takes for a packet of data to get from one designated point to another. This field displays the two mapping modes for latency (fast and interleaved).

4.3.2 Advanced Setup — Configuration

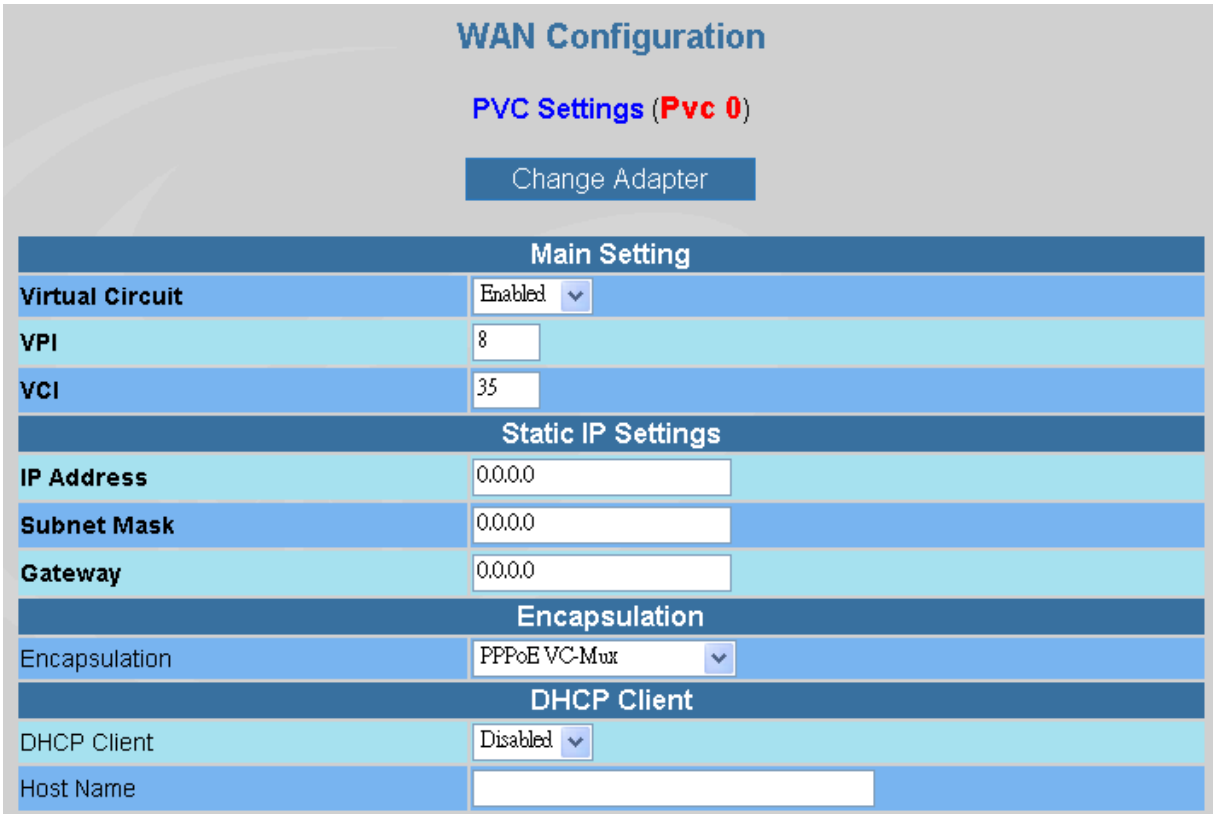
The links under **Configuration** column are associated to the pages that represent the configurations of system and interfaces. These pages can be viewed and modified by both **user** and **admin** accounts.

Note: When any settings are changed, please go to the Save Settings page to save the new setting(s) and reboot the ADSL Router. Changes will not take effect until the settings are saved and the ADSL Router is rebooted. If power is lost before saving, all new configurations since the last save will be lost, even if they were submitted.

4.3.2.1 Configuration—WAN

The **WAN** configuration page allows you to set the configuration for the WAN/ADSL ports. Before you enter the **WAN Configuration** page, you will be asked to select an adapter (PVC0 through PVC7) first.

Once you select the adaptor, then following page will appear.



A. Change Adapter : Click the "Change Adapter" tab to select the PVC Setting. Click "Submit after your choice to view the setting/configurations details.

B. Main Setting :

- Virtual Circuit: Select Enable to activate the current PVC configuration. The current PVC is displayed at the top of the page in parenthesis. Default is Enabled for PVC0 and Disabled for PVC1-PVC7.

- VPI: Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
  - Range for VPI field is 0-255, default is 0.

- VCI: A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
  - Range for VCI field is 0-65535, default is 35.

C. Static IP Settings :

Static IP Settings are for users who have a Static IP Address (WAN side) from their ISP.

- IP Address: This is the static IP Address given by the ISP.

  Range for IP Address is x.x.x.y, where 0 ≦ x≦ 255 and 1 ≦ y≦ 254, default is 192.168.241.101.

- Subnet Mask: This is the subnet mask given by the ISP.

  Range for Subnet Mask is x.x.x.x, where 0 ≦ x≦ 255, default is 255.255.255.0

- Gateway: This is the Gateway given by the ISP.

  Range for Gateway is x.x.x.y, where 0 ≦ x≦ 255 and 1 ≦ y≦ 254, default is 0.0.0.0.

D. Encapsulation :

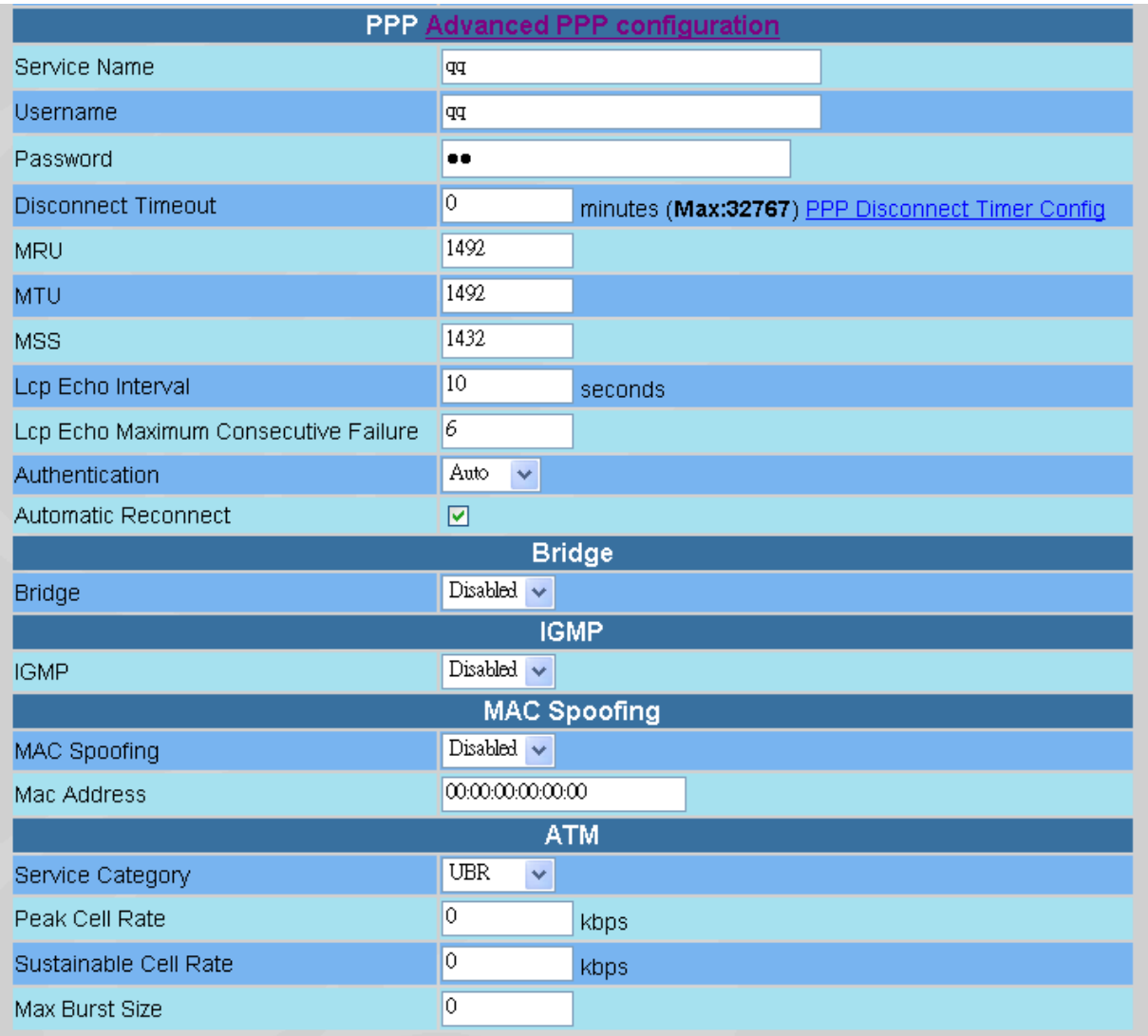
The different types of encapsulation include :

i. PPPoA VC-Mux
ii. PPPoA LLC
iii. 1483 Bridged IP LLC
iv. 1483 Routed IP LLC
v. 1483 Bridged IP VC-Mux
vi. 1483 Routed IP VC-Mux
vii. Classical IP over ATM
viii. PPPoE VC-Mux
ix. PPPoE LLC
x. PPPoE None.

E. DHCP Client :

- DHCP Client: This is to enable or disable (default) the ADSL Router WAN as a DHCP client, where the ISP would be the DHCP server. DHCP Client is generally used in the following encapsulations: 1483 Bridged IP LLC, 1483 Routed IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP VC-Mux, and Classical IP over ATM. This option is for non-static (dynamic) IP addresses.

- Host Name: When DHCP Client is Enabled, copy the ISP recognized Host Name here. The Host Name can be up to 19 characters.



F. PPP "Advanced PPP Configuration" :

The **PPP "Advanced PPP Configuration"** allows you to configure multiple PPP sessions for each PVC. Multiple PPP sessions enables you to set up different connection settings and be able to toggle/choose those settings for each PVC. The ADSL Router can support up to total of 16 PPP sessions, and each PVC can support up to 8 PPP sessions. The multiple PPP sessions may be configured with any combination over 8 PVCs.

- Service Name: The Service Name of the PPP session is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.

- User Name: Enter the PPP user name (provided by the ISP). The User Name can be up to 127 characters.

  Note: You cannot have two different user accounts with the same account name. If a different User Name with an already existing Account ID is submitted, it will replace the previous account with that Account ID. You can have the same User Name and Password for two different accounts (Account ID).

- Password: Enter the PPP password (provided by the ISP). The Password is not needed to delete or modify the account. The Password can be up to 127 characters.

- Disconnect Timeout: The Disconnect Timeout allows you to set the specific period of time, in minutes, to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.

  Note : Range for Disconnect Timeout field is 0-32767, default value is 0.

- MRU: The MRU (Maximum Receive Unit) field indicates the maximum size IP packet that the peer of PPP connection (this device) can receive. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

  Note : Range for MRU field is 0-32767, default value is 1492.

- MTU: Maximum Transmission Unit (MTU) is the largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

  Note : Range for MTU field is 0-32767, default value is 1492.

- MSS: Maximum Segment Size is the largest size of data that TCP will send in a single, unfragmented IP packet. The LAN client and the WAN host will indicate their MSS during the TCP connection handshake.

  Note : Range for MSS field is 0-32767, default value is 1432.

- Lcp Echo Interval: This is the time interval, in seconds, between PPP session connection attempts.

  Note :Range for Lcp Echo Interval field is 0-32767, default value is 10.

- Lcp Echo Maximum Consecutive Failure: This is the number of times a PPP session can fail while trying to connect before stopping. If a PPP session fails this number of times, you must manually reconnect the PPP session.

  Note : Range for Lcp Echo Maximum Consecutive Failure field is 0-32767, default value is 6.

- Authentication: The different types of available authentications are:

    - Auto: When auto is selected, PAP mode will run by default. However, if PAP fails, then CHAP will run as the secondary protocol. This is the default setting.
    - PAP: Password Authentication Procedure. Authentication is done through username and password.
    - CHAP: Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

- Automatic Reconnect: When it is checked, the ADSL Router will reconnect a PPP session when it is terminated by the ISP. If a PPP session is terminated under any other conditions (i.e. by Disconnect Timeout or manual disconnect), the Automatic Reconnect will not reconnect the session. This box is unchecked by default.

G. Bridge :

Bridge: Enable to connect the LAN to the WAN (bridge the two connections). This is available in Bridge Mode only (see Table G). Default is Disabled.

Rx Entity	Packet Class	TTL	Action	Notes
ADSL	IGMP query	1	Relay to Ethernet	
	IGMP report	1	Ignore	
	IGMP leave	1	Ignore	
	General Multicast IP	-	Relay it to Ethernet.	
Ethernet	IGMP query	1	Ignore	
	IGMP report	1	Relay to all ADSL PVC	
	IGMP leave	1	Relay to all ADSL PVC	
	General Multicast IP	-	Ignore	

Table G : Packet process

H. IGMP :

IGMP: IGMP (Internet Group Management Protocol) relay/proxy specification and environment, default is Disabled. IGMP is available in all modes and all encapsulations. Support IGMP proxy/relay function for ADSL Router, based on the following requirement and cases:

- On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The ADSL Router is responsible to relay these IGMP queries to Ethernet.

- End-user multicast application device sends IGMP report while receiving IGMP query or being activated by the user. The ADSL Router should be responsible to proxy (that is, change source IP to ADSL Router's WAN IP) the IGMP report to ADSL WAN side, including all PVCs. The same case is for IGMP leave packet.

- Not necessary to relay multicast routing between two ADSL PVCs or two interfaces in LAN side.

- Special purpose multicast packet (such as RIP 2 packet) should run without Interference.

Note: Before the IGMP mode is enabled; please go to the Miscellaneous Configuration page to enable the IGMP proxy. Otherwise, the IGMP selection will not be valid.

Q: Where can I download the free software to test IGMP?
A: Please go to this link http://manimac.itd.nrl.navy.mil/**MGEN**/

I. MAC Spoofing :

- MAC Spoofing: Enable MAC Spoofing to make a different MAC Address appear on the WAN side. This is also used to solve the scenario where the ISP only recognizes one MAC Address.

  Note : Default is Disabled.

- MAC Address: When MAC Spoofing is enabled, copy the ISP-recognized MAC address here. Format for MAC address is six pairs of hexadecimal numbers (0-9, A-F) separated by colons.

  Note : Default is 00:00:00:00:00:00.

J. ATM :

Asynchronous Transfer Mode: A method of transfer in which data is organized into 53-byte cell units. ATM cells are processed asynchronously in relation to other cells.

- Service Category: This field allows you to select from the following service categories, with UBR as the default.

  - UBR (Unspecified Bit Rate): When configured as UBR, traffic is delivered with best efforts but with no guarantee. This allows for fluctuation in times of temporary increase of available bandwidth. For example, if a PVC with CBR is temporarily inactive, the PVC(s) with UBR will utilize that bandwidth while it is available. UBR is intended for applications that do not require any maximum bound on the transfer delay.

  - CBR (Constant Bit Rate): When a PVC is specified as a CBR, that PVC is guaranteed a certain bandwidth, characterized by the Peak Cell Rate (PCR). The CBR does not have to transmit with a peak cell rate, and when it does, it is only when the bandwidth specified by the PCR is guaranteed.

  - VBR-nrt (Variable Bit Rate - non real time): An PVC enabled with VBR-nrt can transmit a cell only if the PVC has a token available. The PVC accumulates tokens at the rate of the **Sustainable Cell Rate**, and the PVC can only accumulate a maximum of the value specified by **Maximum Burst Size** tokens. When a PVC has a token available, it can transmit cells at the rate of PCR. After a cell is transmitted, the PVC loses the token it has accumulated.

Note: In the case of multiple PVCs, CBR specified PVCs will have higher priority than PVCs with UBR. For example, the CBR PVCs will take their bandwidth and the remaining bandwidth will be split among the UBR PVCs. In the case of total PVC CBR bandwidth exceeding ADSL upstream, the total upstream bandwidth will be shared proportionally to the bandwidth allocated for each CBR PVC.

- Peak Cell Rate: This value specifies the maximum, and in some cases guaranteed, cell rate for CBR and VBR-nrt. Peak Cell Rates are typically measured in Cells/Second, however, the user entered value is in kbps and is then converted by the firmware.

  Note : Range for Peak Cell Rate field is 0-32767, default is 0.

- Sustainable Cell Rate: This is the sustained rate at which a PVC enabled with VBR-nrt can transmit ATM cells. Sustainable Cell Rate (SCR) can be considered as the true reserved bandwidth for a PVC.

  Note :Range for Sustainable Cell Rate field is 0-32767, default is 0.

- Max Burst Size: This is the number of cells a PVC enabled with VBR-nrt can transmit continuously at peak cell rate (PCR).

  Note : Range for Max Burst Size field is 0-32767, default is 0.

A. Example: CBR and UBR :

This example is provided to further explain the dynamics of UBR and CBR and how different PVCs with different service category specifications coexist.

In this example, the ADSL upstream is 900 kbps.

Sample Configuration		
PVC	**Service Category**	**Peak Cell Rate**
0	CBR	400 kbps
1	CBR	800 kbps
2	UBR	N/A
3	UBR	N/A

Scenario	Actual (Adjusted) Bandwidth Usage
PVC0 is busy PVC1 is idle PVC2 and PVC3 are busy	PVC0 uses 400 kbps PVC2 uses 250 kbps PVC3 uses 250 kbps
PVC0 is idle PVC1 is busy PVC2 and PVC3 are busy	PVC1 uses 800 kbps PVC2 uses 50 kbps PVC3 uses 50 kbps
PVC0 is busy PVC1 is busy PVC2 and PVC3 are busy	PVC0 uses 300 kbps PVC1 uses 600 kbps PVC2 uses 0 kbps PVC3 uses 0 kbps

B. Example: VBR-nrt :

This example is provided to further explain the dynamics of VBR-nrt. A PVC has a service category of VBR-nrt with the following parameters:

1. PCR = 400 kbps
2. SCR = 100 kbps
3. MBS = 22 cells (Note that 22 cells * 48 bytes/cell = 1056 bytes)

If the PVC has been idle for a while (meaning it has accumulated a MBS of 22 cells), and it just has two packets of the same size (1000 bytes) to send. It can transmit the first packet of size (1000 bytes) in 20ms: (1000 bytes * 8bit/byte / 4000kbps). Immediately after the first second packet is transmit, it will take about 80ms to transmit the second packet because the PVC can only transmit the second packet at SCR (100kbps).

- Click **"Save Setting"** after configuration/setting to activate your ADSL Router.

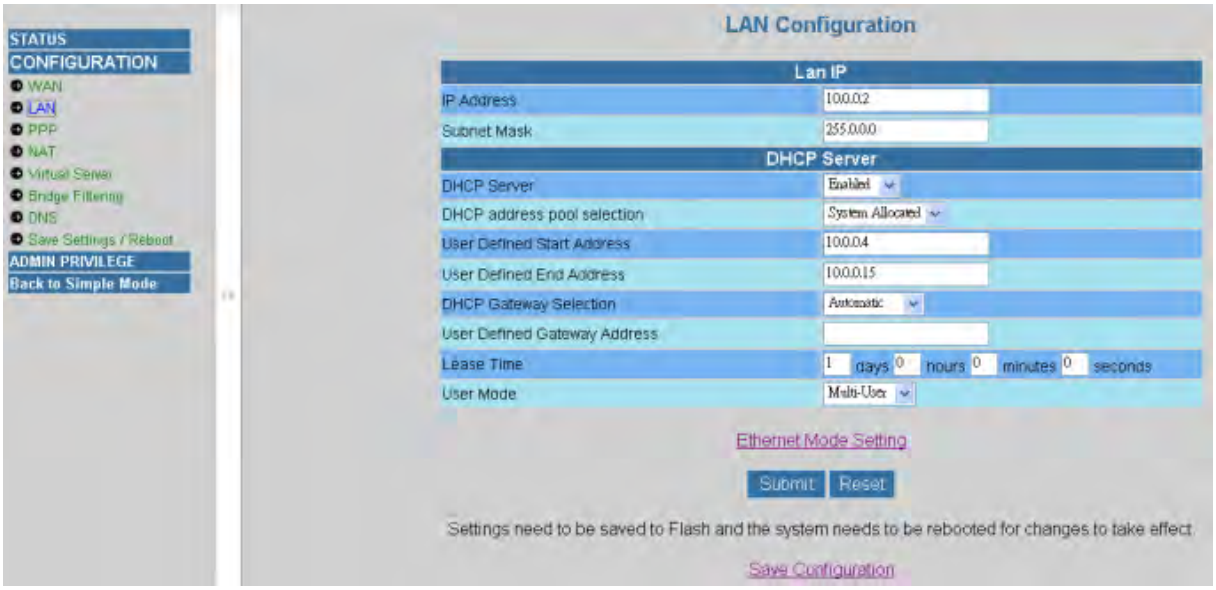
4.3.2.2 Configuration—LAN

The **LAN** configuration allows you to set the configuration for the LAN port.

A. LAN IP :

- LAN IP Address & Subnet Mask: The LAN IP Address is what the computer uses to identify and communicate with the ADSL Router (this is the address you enter in the address bar of Internet Explorer to access these pages). You can change this to another private IP address and subnet mask, such as 192.168.1.2 and 255.255.255.0.

  Note : Range for IP Address and Subnet Mask is x.x.x.x, where 0 ≦ x≦ 255; the default is 10.0.0.2 and 255.0.0.0, respectively.



B. DHCP Server :

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP is controlled by the DHCP Server. The following settings allow you to configure the DHCP server.

- DHCP Server: Select Enabled (default) to activate DHCP Server.

- DHCP Address Pool Selection: Two types of Address Pool selections are available, with System Allocated as the default.

    - **System Allocated:** The DHCP address pool is based on LAN port IP address plus 12 IP addresses. For example, when the LAN IP address is 10.0.0.2; the DHCP address pool the range from 10.0.0.3 to 10.0.0.14.
    - **User Defined:** When User Defined is selected, the DHCP address pool starts at the **User Defined Start Address** and ends at the **User Defined End Address**. The maximum pool size can be 253 IP addresses: 255 total IP addresses – 1 broadcast address – 1 LAN port IP address.

- User Defined Start Address: This is the starting IP address of the DHCP pool for User Defined DHCP Address Pool Selection.

    Note : Range for User Defined Start Address is x.x.x.x, where 0 ≦ x≦ 255, default value is 10.0.0.4.

- User Defined End Address: This is the last IP address in the DHCP pool. User Defined DHCP Address Pool Selection.

    Note : Range for User Defined End Address is x.x.x.x, where 0 x 255, default value is 10.0.0.15.

- DHCP Gateway Selection: The default setting for the DHCP Gateway Selection is Automatic. You can select User Defined and specify User Defined Gateway Address. The DHCP server will issue the User Defined Gateway Address to the LAN DHCP clients.

- User Defined Gateway Address: The purpose for the User Defined Gateway Address is to have two gateway addresses, as the LAN IP Address at the top of the LAN Configuration page is also a gateway address.

- Lease time: The Lease time is the amount of time a network user will be allowed to connect with DHCP server. If all fields are 0, the allocated IP addresses will be effective forever.

    Note : Ranges for Lease Time fields: Days 0-36500, Hours 0-23, Minutes 0-59, Seconds 0-59, default value is 1 days 0 hours 0 minutes 0 seconds.

- User mode: Under the Single User mode, the DHCP server only allocates one IP address to a local PC. Under the Multiple User mode (default), the DHCP server allocates the IP addresses specified by the DHCP address pool.

C. Ethernet Mode Setting :

The **Ethernet Mode** configuration page allows you to set the LAN port into the following modes:

- AutoSense: The ADSL Router will automatically sense which mode to use, selecting between 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, and 10 Mbps Half Duplex. This is the default setting.

- 100 Mbps Full Duplex: Data can be transferred and received simultaneously at the transfer rate of 100 Mega-bits per second.

- 100 Mbps Half Duplex: Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 100 Mega-bits per second.

- 10 Mbps Full Duplex: Data can be transferred and received simultaneously at the transfer rate of 10 Mega-bits per second.

- 10 Mbps Half Duplex: Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 10 Mega-bits per second.

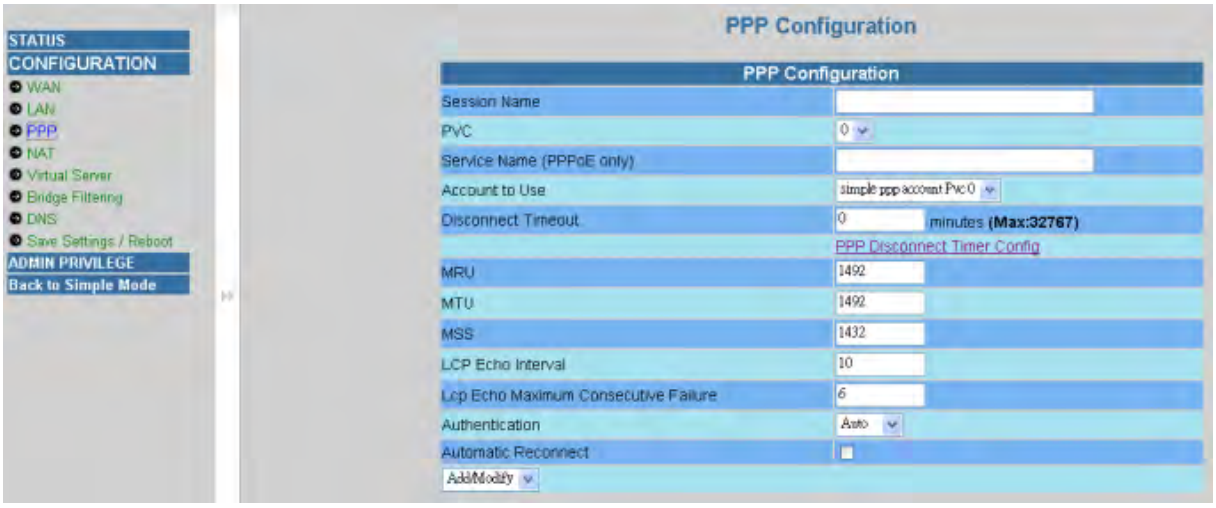
  Note : Default is "AutoSense".

- Save Configuration : Clicking this will link you to the Save Settings / Reboot page.

4.3.2.3 Configuration—PPP

A. PPP Configuration :

The **PPP Configuration** page allows you to configure multiple PPP sessions for each PVC. Multiple PPP sessions enables you to set up different connection settings and be able to toggle/choose those settings for each PVC. The ADSL Router can support up to total of 16 PPP sessions, and each PVC can support up to 8 PPP sessions. The multiple PPP sessions may be configured with any combination over 8 PVCs.



- Session Name: This field allows you to enter a Session Name. This is user defined to help distinguish different session for different PPP accounts and different PVCs.
- PVC: This field allows you to choose the specific PVC for the PPP session.
- Service Name: The Service Name of the PPP session is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.
- Account to Use: You must select an account created in PPP Account Configuration page here.
- Disconnect Timeout: The Disconnect Timeout allows you to set the specific period of time, in minutes, to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.

  Note : Range for Disconnect Timeout field is 0-32767, default value is 0.

- PPP Idle Timer Config: This will link you to the PPP Disconnect Timer Configuration page.

- MRU: The MRU (Maximum Receive Unit) field indicates the maximum size IP packet that the peer of PPP connection (this device) can receive. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

  Note : Range for MRU field is 0-32767, default value is 1492.

- MTU: Maximum Transmission Unit (MTU) is the largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

  Note : Range for MTU field is 0-32767, default value is 1492.

- MSS: Maximum Segment Size is the largest size of data that TCP will send in a single, unfragmented IP packet. The LAN client and the WAN host will indicate their MSS during the TCP connection handshake.

  Note : Range for MSS field is 0-32767, default value is 1432.

- Lcp Echo Interval: This is the time interval, in seconds, between PPP session connection attempts.

  Note :Range for Lcp Echo Interval field is 0-32767, default value is 10.

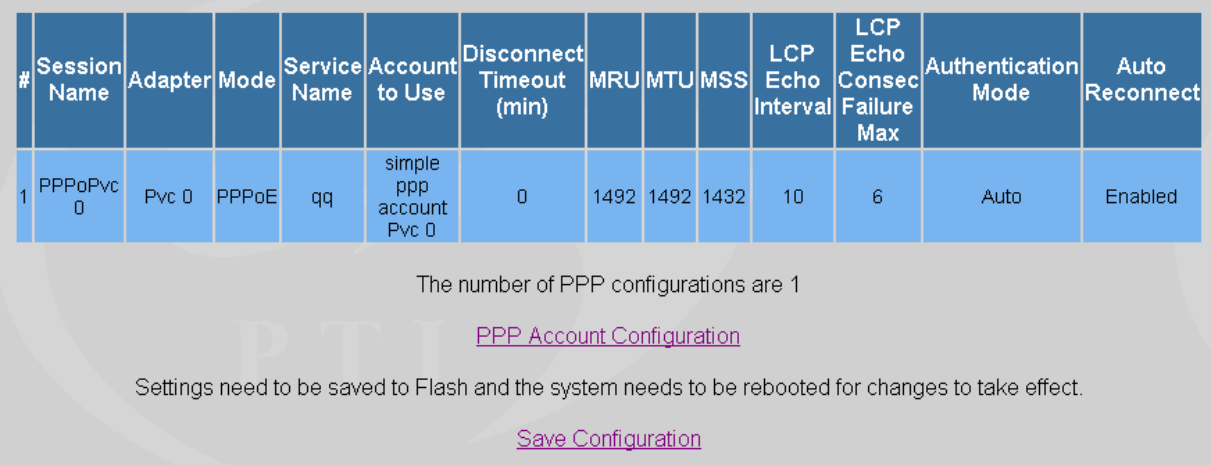
- Lcp Echo Maximum Consecutive Failure: This is the number of times a PPP session can fail while trying to connect before stopping. If a PPP session fails this number of times, you must manually reconnect the PPP session.

  Note : Range for Lcp Echo Maximum Consecutive Failure field is 0-32767, default value is 6.

- Authentication: The different types of available authentications are:

  - Auto: When auto is selected, PAP mode will run by default. However, if PAP fails, then CHAP will run as the secondary protocol. This is the default setting.
  - PAP: Password Authentication Procedure. Authentication is done through username and password.
  - CHAP: Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

- Automatic Reconnect: When it is checked, the ADSL Router will reconnect a PPP session when it is terminated by the ISP. If a PPP session is terminated under any other conditions (i.e. by Disconnect Timeout or manual disconnect), the Automatic Reconnect will not reconnect the session. This box is unchecked by default.



#	Session Name	Adapter	Mode	Service Name	Account to Use	Disconnect Timeout (min)	MRU	MTU	MSS	LCP Echo Interval	LCP Echo Consec Failure Max	Authentication Mode	Auto Reconnect
1	PPPoPvc 0	Pvc 0	PPPoE	qq	simple ppp account Pvc 0	0	1492	1492	1432	10	6	Auto	Enabled

The number of PPP configurations are 1

PPP Account Configuration

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

Save Configuration

Example : **Create a PPP session and connect it to the ISP?**
To create and connect a PPP session, follow the steps below:

- First you must create a PPP account. To do this, go to PPP Configuration page and click on PPP Account Configuration. Enter the appropriate Acct ID, User Name, and Password, make sure Add/Modify is currently selected in the dropdown menu, and click Submit.

- Got back to the PPP Configuration Page by clicking Go back to PPP Configuration. Type in an appropriate Session Name and select the account you just created in the Account to Use dropdown menu. Everything else has default values, which you can modify to suit your needs. Make sure Add/Modify is currently selected in the dropdown menu, and click Submit.

- The PPP session has been created. Now you must go to the PPP Status page, select the connection (session), and click Execute. The PPP session should then connect.

- Save Configuration : Clicking this will link you to the Save Settings / Reboot page.

B. PPP Account Configuration :

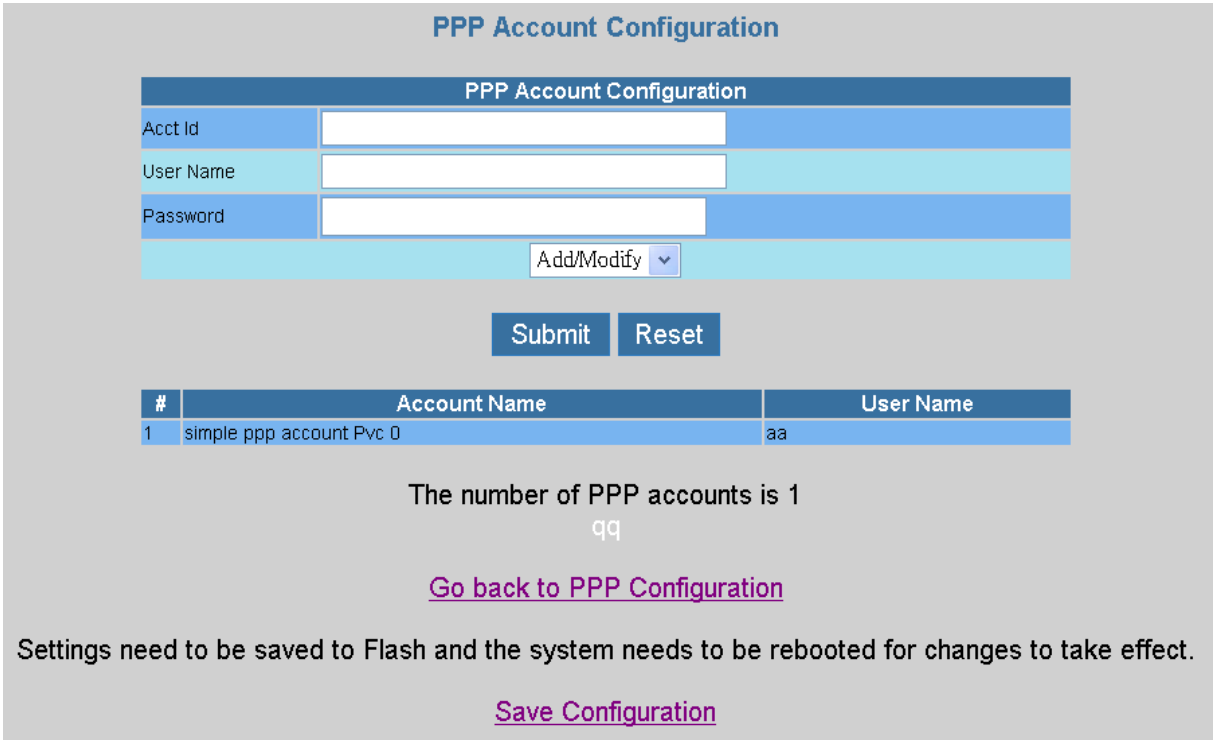
To begin PPP Session configuration, you must first go to the **PPP Account Configuration** page (below) to set up an account. The link to this page can be found on the **PPP Configuration** page. On the **PPP Account Configuration** page, you must configure the Account ID, User Name and Password.

- Account ID: This field allows you to create an account ID to help distinguish different accounts, up to 16 maximum. The Account ID can be up to 31 characters.

- User Name: Enter the PPP user name (provided by the ISP). The User Name can be up to 127 characters.

> *Note: You cannot have two different user accounts with the same account name. If a different User Name with an already existing Account ID is submitted, it will replace the previous account with that Account ID. You can have the same User Name and Password for two different accounts (Account ID).*

- Password: Enter the PPP password (provided by the ISP). The Password is not needed to delete or modify the account. The Password can be up to 127 characters.
- PPP Account Configuration Status table will be displayed at the bottom of this page to show all the accounts (Table headings: Account Name and User Name). The status table does not display the password.
- The Number of PPP Accounts: This field displays the total number of PPP Accounts entered.
- Save Configuration: Clicking this will link you to the Save Settings / Reboot page.


PPP Account Configuration
PPP Account Configuration
Acct Id
User Name
Password
Add/Modify
Submit
Reset
Account Name User Name
1 simple ppp account Pvc 0 aa
The number of PPP accounts is 1
qq
Go back to PPP Configuration
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

C. PPP Disconnect Timer Configuration :

The PPP Disconnect Timer Configuration page enables you to configure what action will bring a PPP Session out of the Idle state (disconnected state) and reset the Idle Timer. This is done by specifying criteria contained in packets, namely IP Protocol and Port. The Idle Timer refers to the Disconnect Timeout, specified on the PPP Configuration page.

The PPP Idle Timer is recommended to be disabled (**Disconnect Timeout** = 0 on PPP Configuration page) if you want an always on connection. **PPP Disconnect Timer Configuration** is intended for users who do not desire an always on connection and/or their ISP charge by connection time.

I. Enable/Disable Idle Timer Filter :

- **All Traffic will reset Idle Timer (ignore filter below):** Selecting this option will disable the PPP Idle Timeout filter and allow any traffic through any protocol or port to reset the idle timer. The only dependency is that the traffic must correspond with the Filter Application (Inbound and/or Outbound). For example, if **Outbound Traffic Only** is selected, only traffic in the outbound direction will reset the idle timer. When this option is selected, all user configured criteria (displayed in the filter table) is bypassed.

- **Only filtered traffic will reset the Idle Timer (use filter below):** Selecting this option will enable the PPP Idle Timeout filter and only allow traffic specified in the filter table to reset the idle timer. The traffic specified in the filter table must also correspond with the Filter Application selection. For example, outbound traffic with criteria matching that of the filter table will only be allowed to pass if either **Outbound Traffic Only** or **Inbound and Outbound Traffic** is selected.

  Note: PPP reconnect on WAN access must be enabled for the Idle Timer to reconnect a PPP Session when a request is made from the LAN to the WAN.

- Click **"Execute"** to activate your setting.

II. Apply Filter :

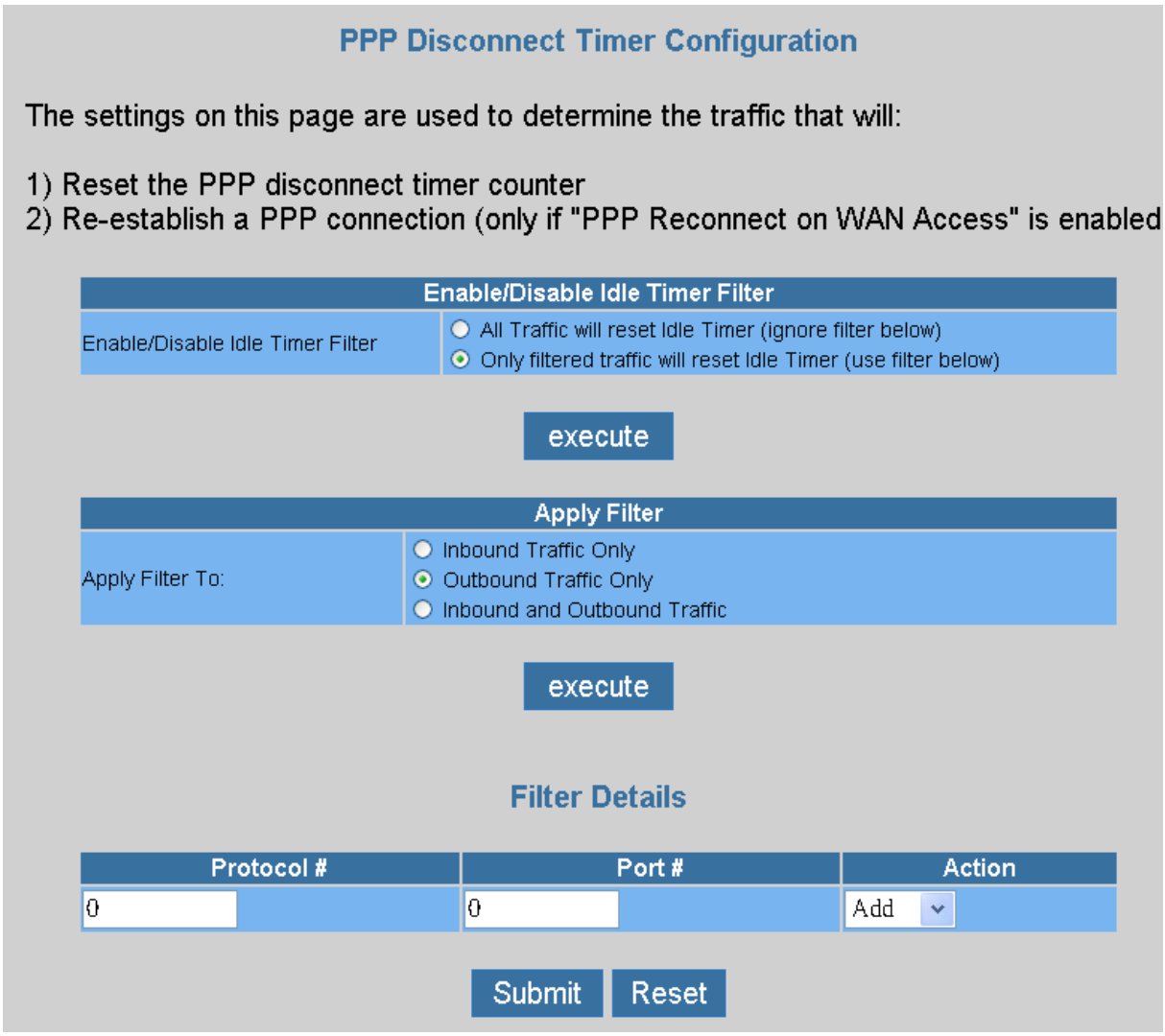
The Filter Application consists of three options that determine which sources (LAN and/or WAN) will be able to reset the Idle Timer and reconnect the PPP session.

- **Inbound Traffic Only:** Selecting this option will allow PPP requests from the WAN side to reset the **Disconnect Timeout** timer. Note that requests from the WAN side cannot bring a PPP Session out of Idle state. This is because when a PPP Session is in Idle state, the connection is down (if they match the filter table criteria).

- **Outbound Traffic Only:** When this option is selected (default), PPP sessions can only be activated (Idle Timeout) when a request is made on the LAN side to the WAN side. The disconnect timer will reset when outbound traffic is detected (if they match the filter table criteria).

- **Inbound and Outbound Traffic:** Selecting this will allow both WAN and LAN source packets to reset the idle timer.

- Click **"Execute"** to activate your setting.



III. Filter Details :

The table displayed in the Filter Details section of the page shows all the current Idle Filters. Traffic must match the criteria of one of these filters in order to cause an Idle Timeout, unless **All Traffic will reset Idle Timer** is selected. As a default and starting point for configuration, WWW browsing (HTTP), FTP, and Telnet related packets are part of the filter table.

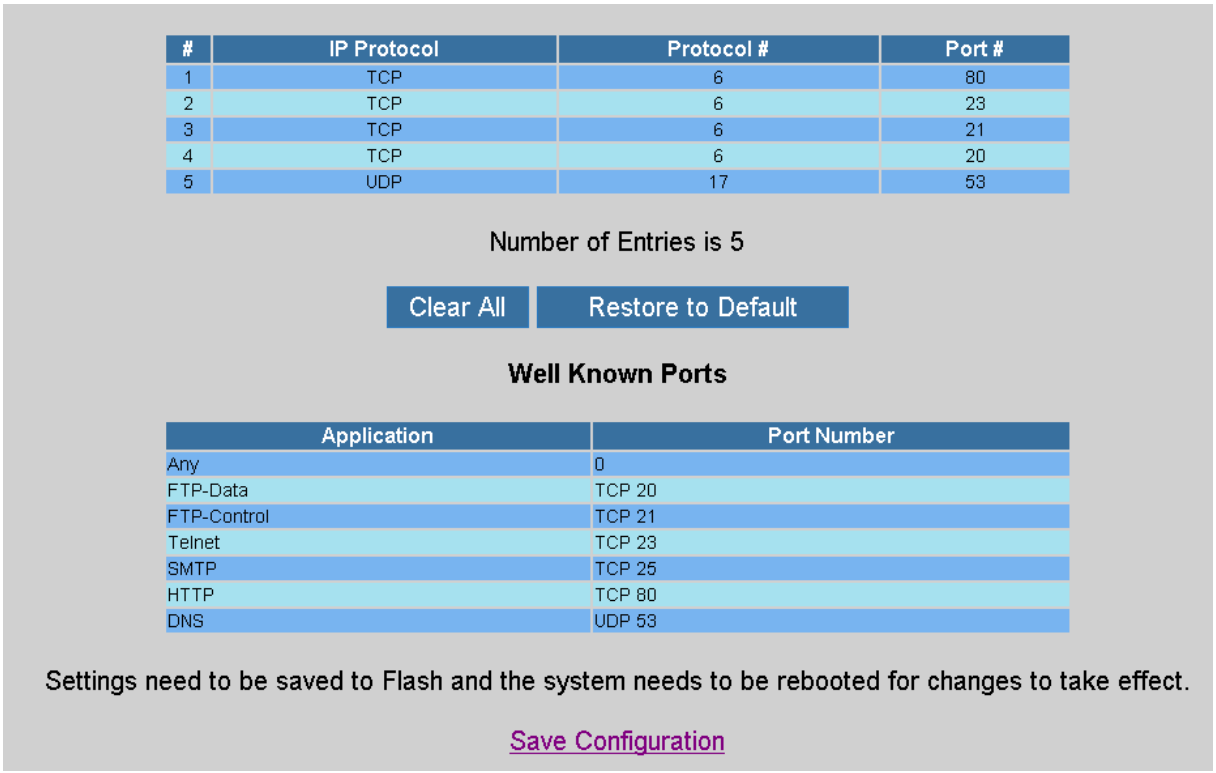
- **IP Protocol:** This is the IP Protocol name corresponding to the Protocol Number.

- **Protocol #:** This is the IP protocol (number) through which the PPP session can be activated. The Protocol Numbers for filters are:

  - TCP Protocol Number: 6
  - UDP Protocol Number: 17
  - ICMP Protocol Number: 1
  - IGMP Protocol Number: 2

- Port #: This is the Port through which the PPP session can be activated. The default filters are:
    - HTTP TCP Port: 80
    - FTP TCP Port: 20 and 21
    - Telnet TCP Port: 23
    - DNS UDP: 53

- Action: You can add a rule by entering the appropriate information, selecting Add on the Action dropdown menu, and clicking Submit. To delete an entry, you can enter the information of an entry that already exists on the table, select Delete on the Action dropdown menu, and click Submit.



#	IP Protocol	Protocol #	Port #
1	TCP	6	80
2	TCP	6	23
3	TCP	6	21
4	TCP	6	20
5	UDP	17	53

Number of Entries is 5

Clear All | Restore to Default

Well Known Ports

Application	Port Number
Any	0
FTP-Data	TCP 20
FTP-Control	TCP 21
Telnet	TCP 23
SMTP	TCP 25
HTTP	TCP 80
DNS	UDP 53

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

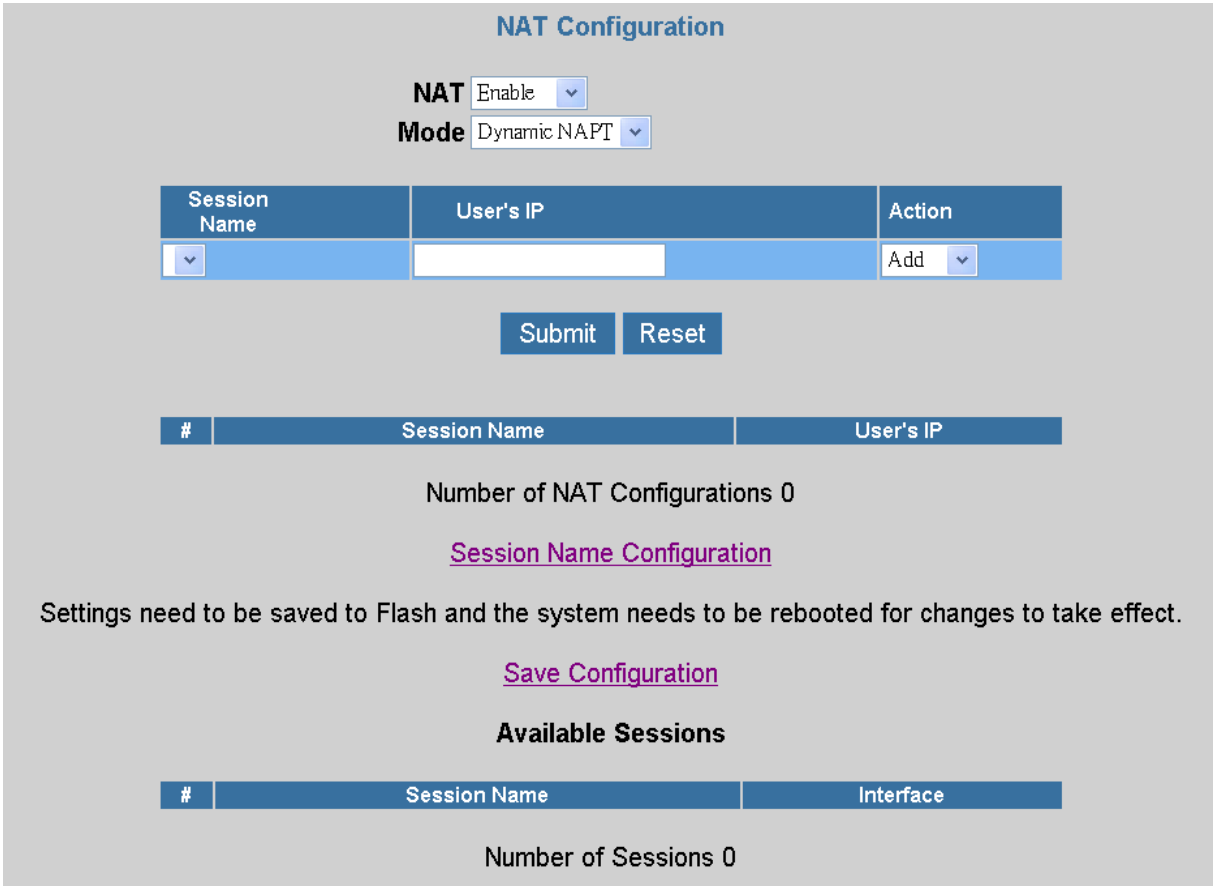
Save Configuration

4.3.2.4 Configuration—NAT

The **NAT Configuration** page allows you to set the configuration for the Network Address Translation. The NAT module provides Dynamic Network Address and Port Translation (**Dynamic NAPT**) capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP addresses and the Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

When **Dynamic NAPT** is chosen (default), there is no need to configure the NAT Session and NAT Session Name Configuration.

I. NAT Configuration :



- **NAT:** Use this field to Enable/Disable NAT. Default is Enable.
- **Mode:** Options for the NAT dropdown menu are:
  - NAT: Static peer-to-peer mode (1x1).
  - NAPT: Static multiple mapping mode (1xN).
  - Dynamic NAPT: Dynamic multiple mapping mode (NxN). This is the default setting.

- **Session Name:** This field allows you to select the session from the configured NAT Session Name Configuration.

- **User's IP:** This field allows you to assign the IP address to map the corresponding NAT/NAPT sessions.

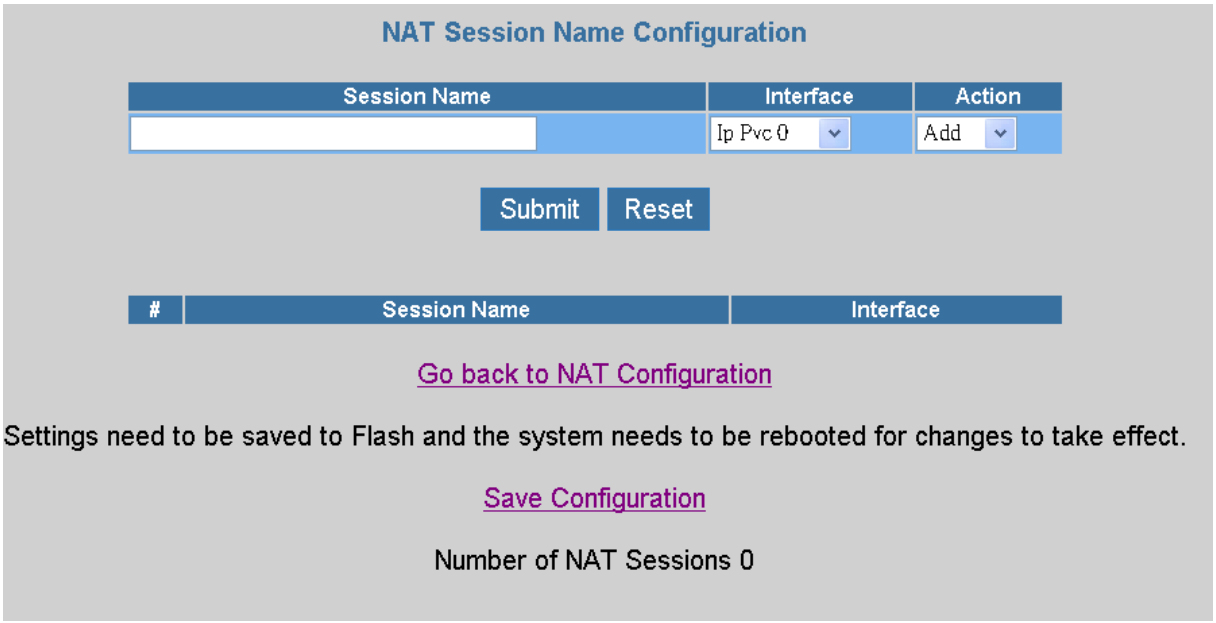
- **Number of NAT Configurations:** This field displays the total number of NAT Sessions entered.

  Note: NAT allows only one entry (User IP) per session, while NAPT allows many entries (User IPs) per session.

- **Available Sessions:** This table will be displayed at the bottom of the page to show all the available Session Names with their corresponding WAN Interface.

- **Number of Sessions:** This field displays the total number of NAT Sessions entered.

II. NAT Session Name Configuration :



- **Session Name:** This field allows you to enter a Session Name to help distinguish different NAT Sessions for different interfaces among different PPP sessions and PVCs. The Session Name can be up to 31 characters, and there can be up to 16 different NAT session names.

- **Interface:** This field allows you to choose specific WAN Interfaces (PVC or PPP Session) for NAT Session. The options for this field are PVC0 ... PVC7 and any PPP session that was created by the user.

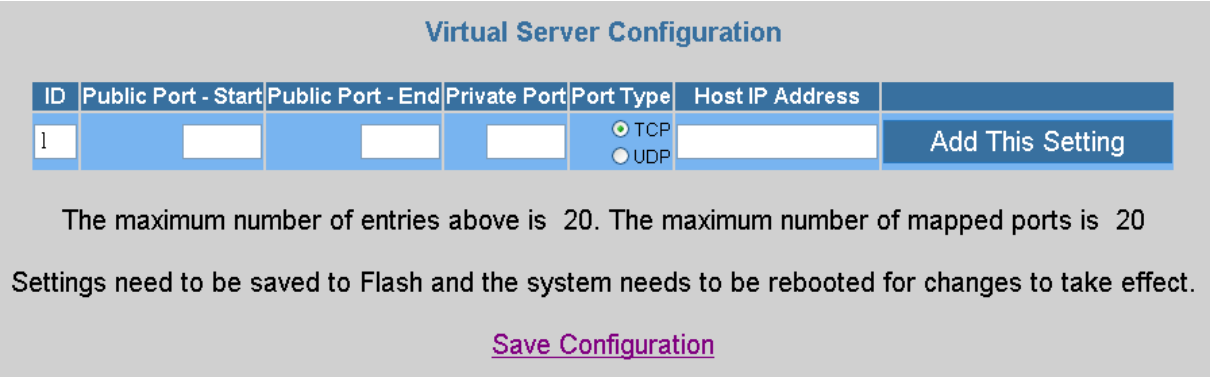
- **NAT Session Name Status:** This table is displayed at the bottom of this page to show all the NAT Session Names with their corresponding WAN Interfaces.

4.3.2.5 Configuration – Virtual Server

Virtual Servers are used for port forwarding from the WAN to LAN networks.

The **Virtual Server Configuration** page allows you to set the configuration of the Virtual Server. All UDP/TCP ports are protected from intrusion. If any specific local PCs need to be mapped to the UDP/TCP port on WAN side, please input the mappings here.

Note :There can be up to 20 different Virtual Server Configurations.


Virtual Server Configuration
ID
Public Port - Start
Public Port - End
Private Port
Port Type
Host IP Address
1
TCP
UDP
Add This Setting
The maximum number of entries above is 20. The maximum number of mapped ports is 20
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

- ID: This is the ID number corresponding to the Virtual Server configuration.
- Public Port - Start: This field allows you to enter the port number of the Public Network (WAN or external network). If you are entering a range of ports, this is the first port.
- Public Port - End: This field represents the last port number in a port range. If you only want one port number (no port range), simply enter the same number here as in the
- Public Port – Start field.

  Note : The maximum number of the mapped Port is 20.

- Private Port: This field allows you to enter the port number of the Private Network (LAN or internal network). In most cases, the private port number is same as public port number. This port number cannot be seen from the WAN side.
- Host IP Address: This field allows you to enter the private network IP address for the particular server. Well-known TCP/IP ports are listed in Table below:

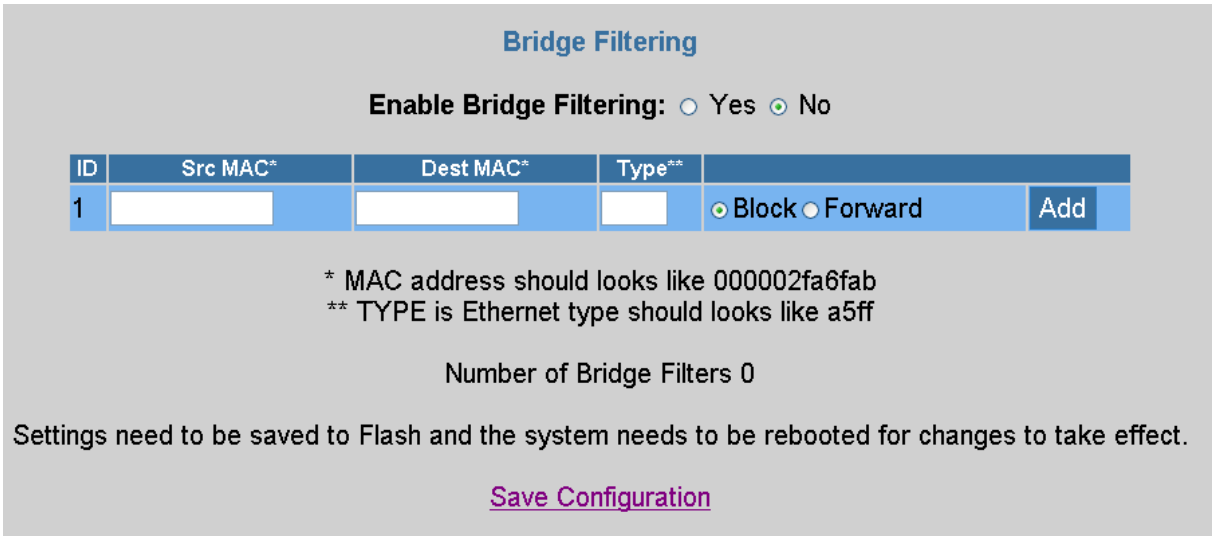
Port	Protocol	TCP	UDP
20	File Transfer Protocol (FTP) Data	X	
21	FTP Commands	X	
23	Telnet	X	
25	SMTP	X	
43	Whois	X	
53	Domain Name System (DNS)	X	X
69	Trivial File Transfer Protocol (TFTP)		X
70	Gopher	X	
79	Finger	X	
80	HTTP	X	
110	POP3	X	
111	SUN Remote Procedure Call (RPC)		X
115	SFTP	X	
119	Network News Transfer Protocol (NNTP)	X	
123	Network Time Protocol (NTP)	X	X
144	News	X	
161	Simple Network Management Protocol (SNMP)		X
162	SNMP traps		X
179	Border Gateway Protocol (BGP)	X	
443	Secure HTTP (HTTPS)	X	
513	rlogin	X	
514	rexec	X	
517	talk	X	X
518	ntalk	X	X
520	Routing Information Protocol (RIP)		X
1701	Layer 2 Tunneling Protocol (L2TP)		X
2000	Open Windows	X	X
2049	Network File System (NFS)	X	
6000	X11	X	X

4.3.2.6 Configuration – Bridge Filtering

Bridge Filtering allows packets to be forwarded or blocked, depending on the MAC address. The **Bridge Filtering** configuration page allows you to set the configuration of MAC filtering.

There can be up to 4 different Bridge Filtering configurations.

- Source MAC: This is the Source MAC to block or from which to forward. See the next page for instructions on how to configure this. The Source MAC must consist of 12 hexadecimal characters.
- Destination MAC: This is the Destination MAC to block or to forward to. See the next page for instructions on how to configure this. The Destination MAC must consist of 12 hexadecimal characters.
- Type: Enter the hexadecimal number for the Ethernet type field in Ethernet_II packets. For example, 0800 is for IP protocol. The Type must consist of 4 hexadecimal characters.
- Block: When block is selected, everything from the Source MAC with destination MAC will be blocked.
- Forward: When forward is selected, everything from the Source MAC will be forwarded to the Destination MAC.


Bridge Filtering
Enable Bridge Filtering: Yes No
ID
Src MAC*
Dest MAC*
Type**
1
Block Forward
Add
* MAC address should looks like 000002fa6fab
** TYPE is Ethernet type should looks like a5ff
Number of Bridge Filters 0
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

Example :

Q1 : How do I forward packets with MAC address 000002fa6fab to destination MAC 000003dc8faa through IP protocol?

ANS : First go to the **Bridge Filtering** page under **Configuration**. Then type 000002fa6fab in the **ID Source MAC** field, 000003dc8faa in the **Destination MAC** field, and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Forward** and click **Submit**.

Q2: How do I block packets from MAC address 000002fa6fab through IP protocol?

ANS : First go to the **Bridge Filtering** page under **Configuration**. Then type 000002fa6fab in the **ID Source MAC** field and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Block** and click **Submit**.

Q3: How do I block incoming packets with destination MAC address 000003dc8faa through IP protocol?

ANS : First go to the **Bridge Filtering page** under **Configuration**. Then type 000003dc8faa in the **Destination MAC** field, and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Block** and click **Submit**.

4.3.2.7 Configuration—DNS

The **DNS Configuration** page allows you to set the configuration of the DNS proxy.

For the DHCP requests from local PCs, the DHCP server will set the LAN port IP as the default DNS server. Thus, all DNS query messages will come into LAN port first. The DNS proxy on the ADSL Router records the available DNS servers and forwards DNS query messages to one of DNS servers.

- DNS Proxy Enable/Disable: When the DNS Proxy is Disabled, the LAN port does not process the DNS query message. For the DHCP requests from local PCs, the DHCP server will set the user-configured DNS server as the DNS server. Then all DNS query messages will be directly sent to the DNS servers. DNS Proxy is enabled by default.

- Auto Discovered: When enabled (default), the DNS proxy will store the DNS server IP addresses obtained from DHCP client or PPP into the table. All DNS query messages will be sent to the dynamically obtained DNS server. Select this option when the DNS Server address is unknown but provided (automatically) by the ISP.

- User Configured: When enabled, the DNS proxy will use the user-configured DNS server. All DNS query messages will be sent to the DNS server. Enter the DNS IP in the DNS Server field. Select this option when the DNS Server address assigned by the ISP is known. User Configured is disabled by default.

- Auto Discovery + User Configured: Selecting both options will cause the DNS proxy's table to have all the IP addresses of dynamically obtained and user configured DNS servers.

- DNS Server: This is the user defined DNS server URL name and IP. Default is Disabled.

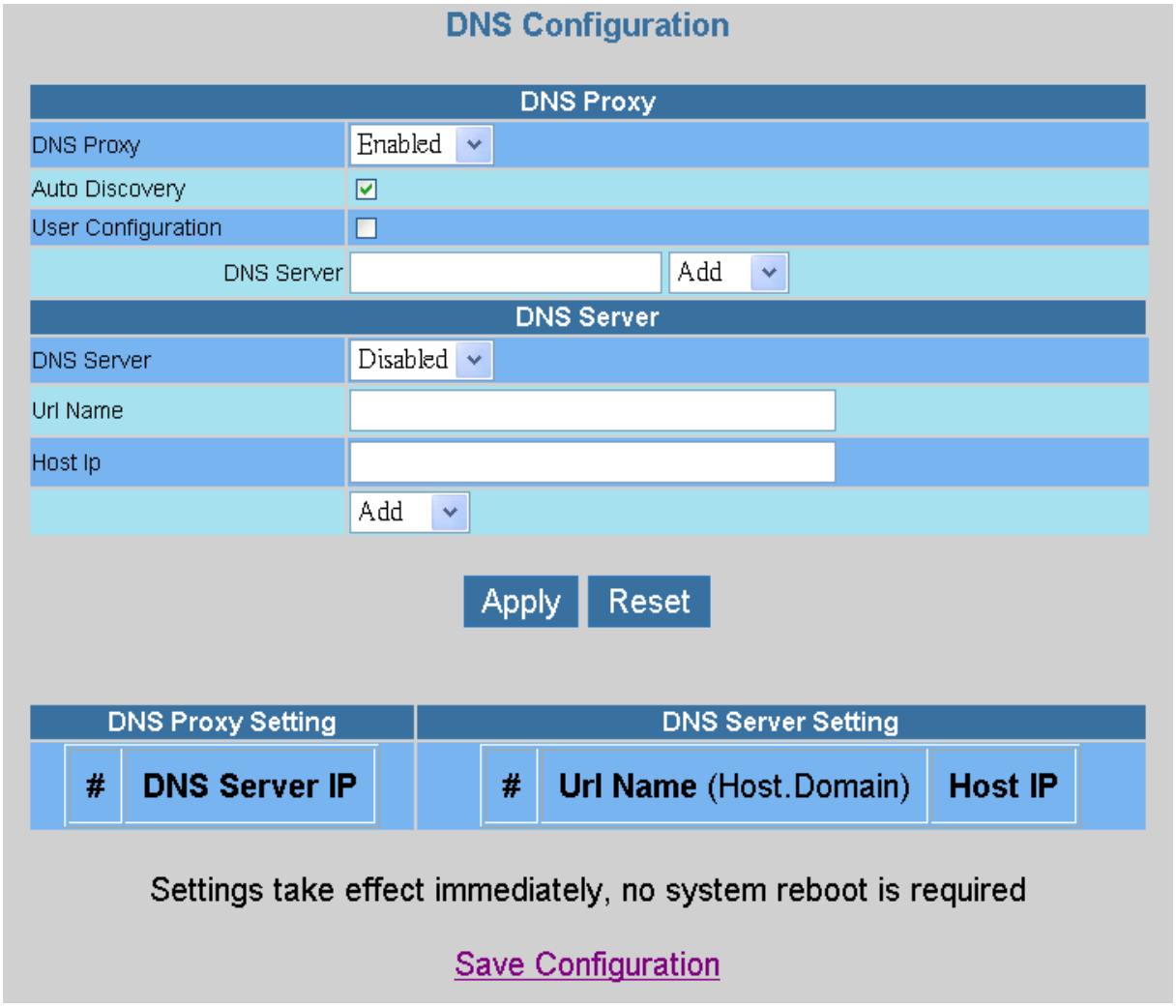
- URL Name (Add/Delete): This is the URL name for the DNS server. This can be up to 255 characters.

- Host IP (Add Only): This is the IP address of the DNS Server.

- DNS Proxy Setting: This is a table of all DNS server IP addresses.

- DNS Server Setting: This is a table of all DNS sever URL names.

- Save Configuration: Clicking this will link the user to the Save Settings / Reboot page.

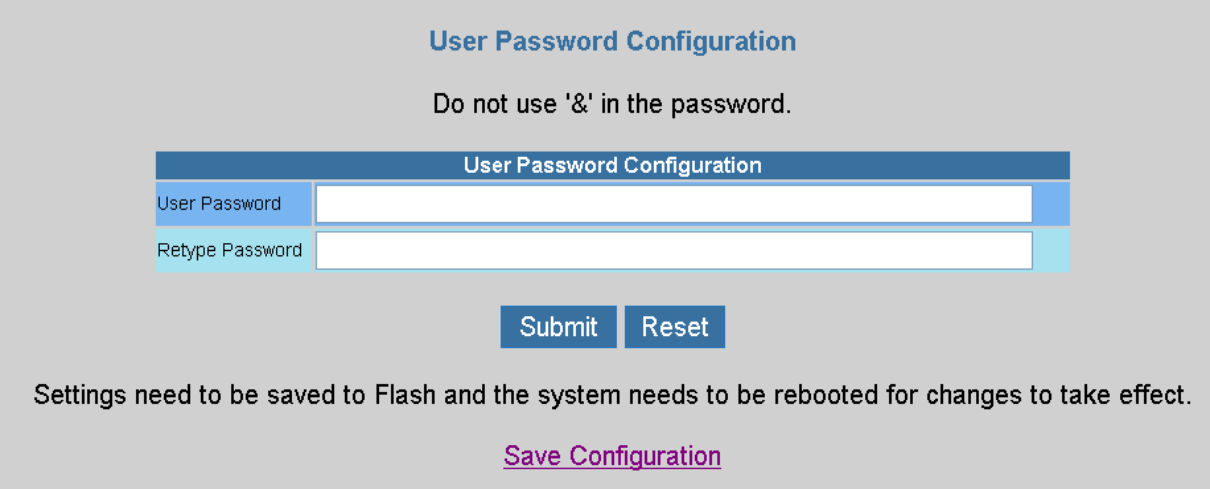

DNS Configuration
DNS Proxy
DNS Proxy
Enabled
Auto Discovery
User Configuration
DNS Server
Add
DNS Server
DNS Server
Disabled
Url Name
Host Ip
Add
Apply
Reset
DNS Proxy Setting
DNS Server IP
DNS Server Setting
Url Name (Host.Domain) Host IP
Settings take effect immediately, no system reboot is required
Save Configuration

4.3.2.8 Configuration – User Password Configuration

The **User Password Configuration** page allows the **user** or **admin** to set the password for the user account.

The User Password can be up to 65 characters (excluding ‘&’).

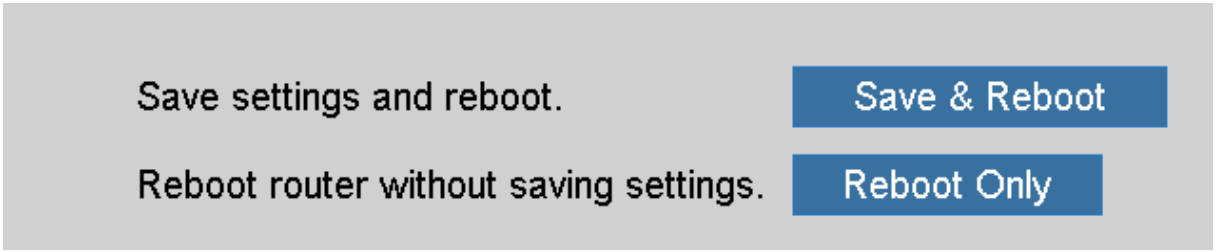
Note: User Account cannot be used to access FTP server.


User Password Configuration
Do not use '&' in the password.
User Password Configuration
User Password
Retype Password
Submit
Reset
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

- Save Configuration: Clicking this will link the user to the Save Settings / Reboot page.

4.3.2.9 Configuration – Save Setting/Reboot

The **Save Settings / Reboot** page allows you to either save the new configuration to the flash and reboot the ADSL Router or simply reboot the ADSL Router without saving changes.



- Save & Reboot: Click this to apply all changes.
- Reboot Only: Do this to discard all changes since last save.

After either one of these buttons are clicked, the ADSL Router will do the following:

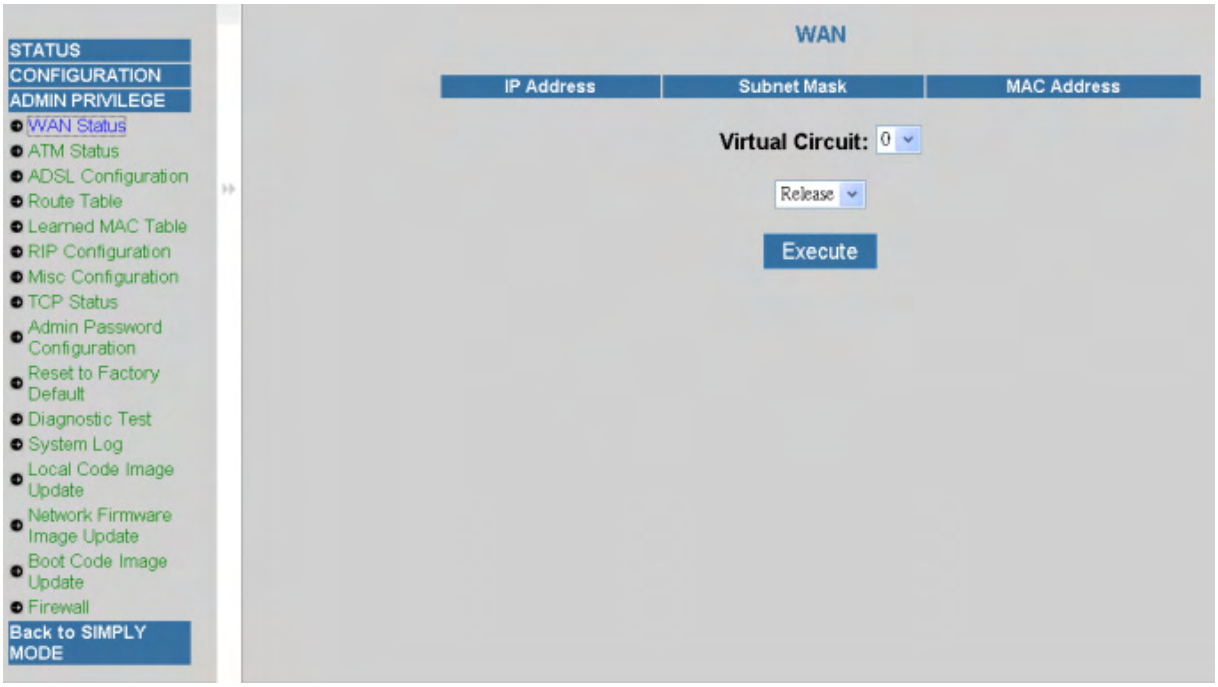
I. **Save & Reboot:** Two pages will appear after pressing this button. The first one states: "Your settings are being saved and the modem being rebooted. Save reboot in progress, please wait…." Followed by "Your settings have been saved and the modem has rebooted. Done"

II. **Reboot Only:** Two pages will appear after pressing this button. The first one states: "The modem is being rebooted. Reboot in progress, please wait…." Followed by "The modem is being rebooted. Done."

4.3.3 Advanced Setup – Admin Privilege

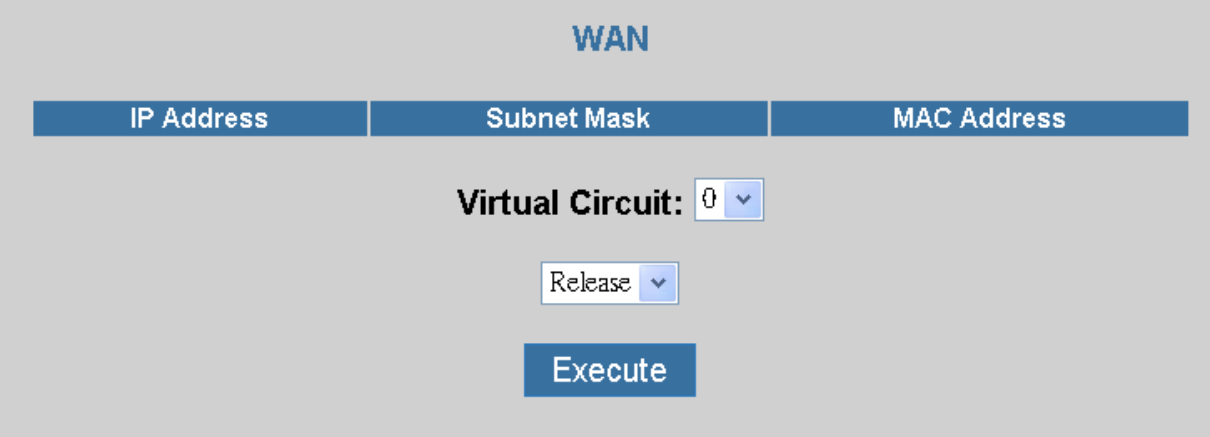
The links under **Admin Privilege** are only accessible when user is logged in as **Admin**.

Regular user account does not have authorization to view or alter the content on the pages in the **Admin Privilege** section.



4.3.3.1 Admin Privilege – WAN Status

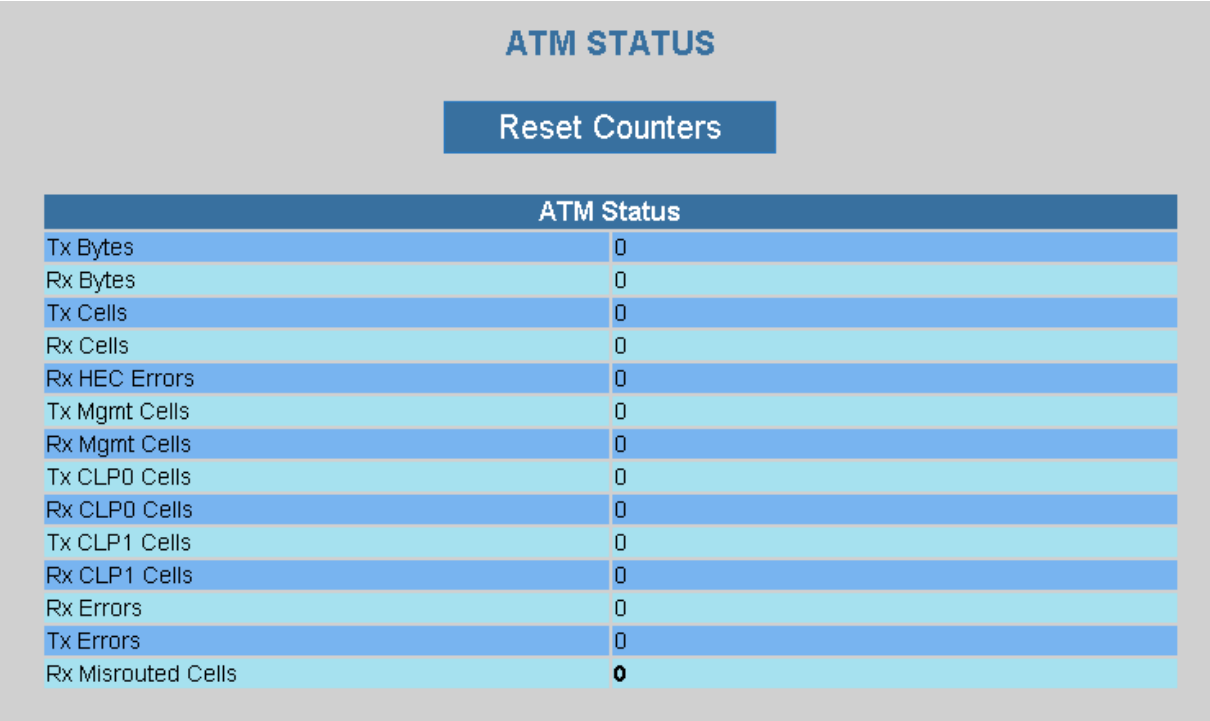
The **WAN Status** page shows the information and status of WAN PVCs.



- WAN: This field displays the IP address, Subnet Mask and MAC address for the WAN (ADSL) interface. Use the Virtual Circuit selection to select different PVCs for status display.
- Virtual Circuit: Select the Virtual Circuit that you want to release/renew, select the appropriate option on the menu dropdown and click Execute.

4.3.3.2 Admin Privilege – ATM Status

The **ATM Status** page shows all the statistics information of ATM cells. This page contains information that is dynamic and will refresh every 2 seconds.

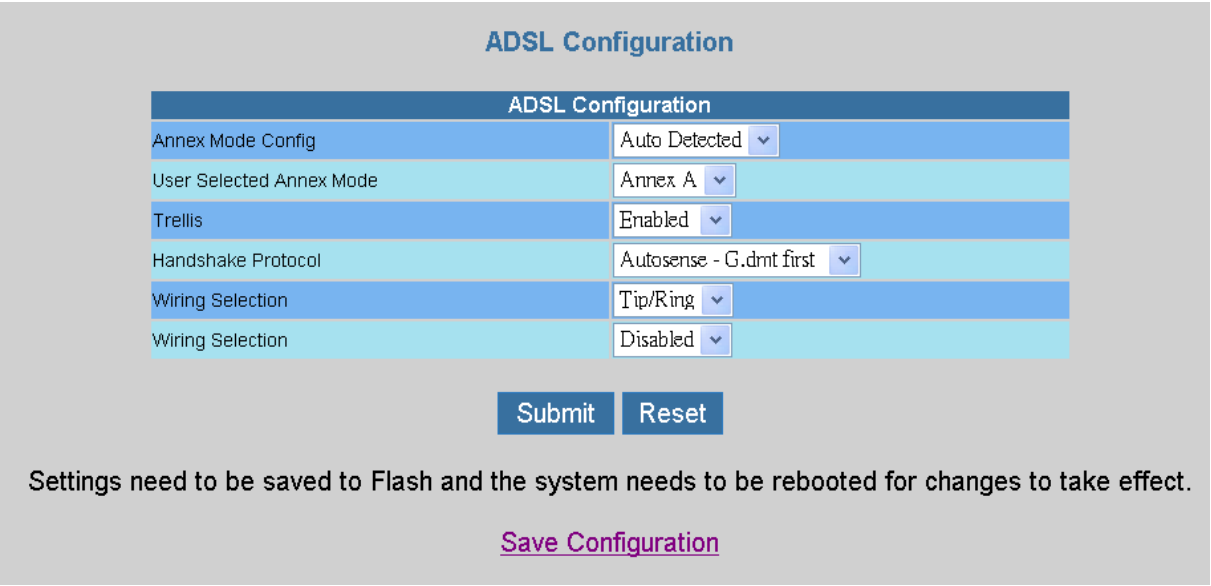


- Reset Counters: This button allows user to reset the ATM Status counter.
- ATM Status Fields: Tx Bytes, Rx Bytes, Tx Cells, Rx Cells, Rx HEC Errors, Tx Mgmt Cells, Tx CLP0 Cells, Rx CLP0 Cells, Tx CLP1 Cells, Rx CLP1 Cells, Rx Errors, Tx Errors, and Rx Misrouted Cells.

  Note: For more information on HEC, Cell, CLP0, and CLP1, please refer to Appendix F: Glossary.

4.3.3.3 Admin Privilege – ADSL Configuration

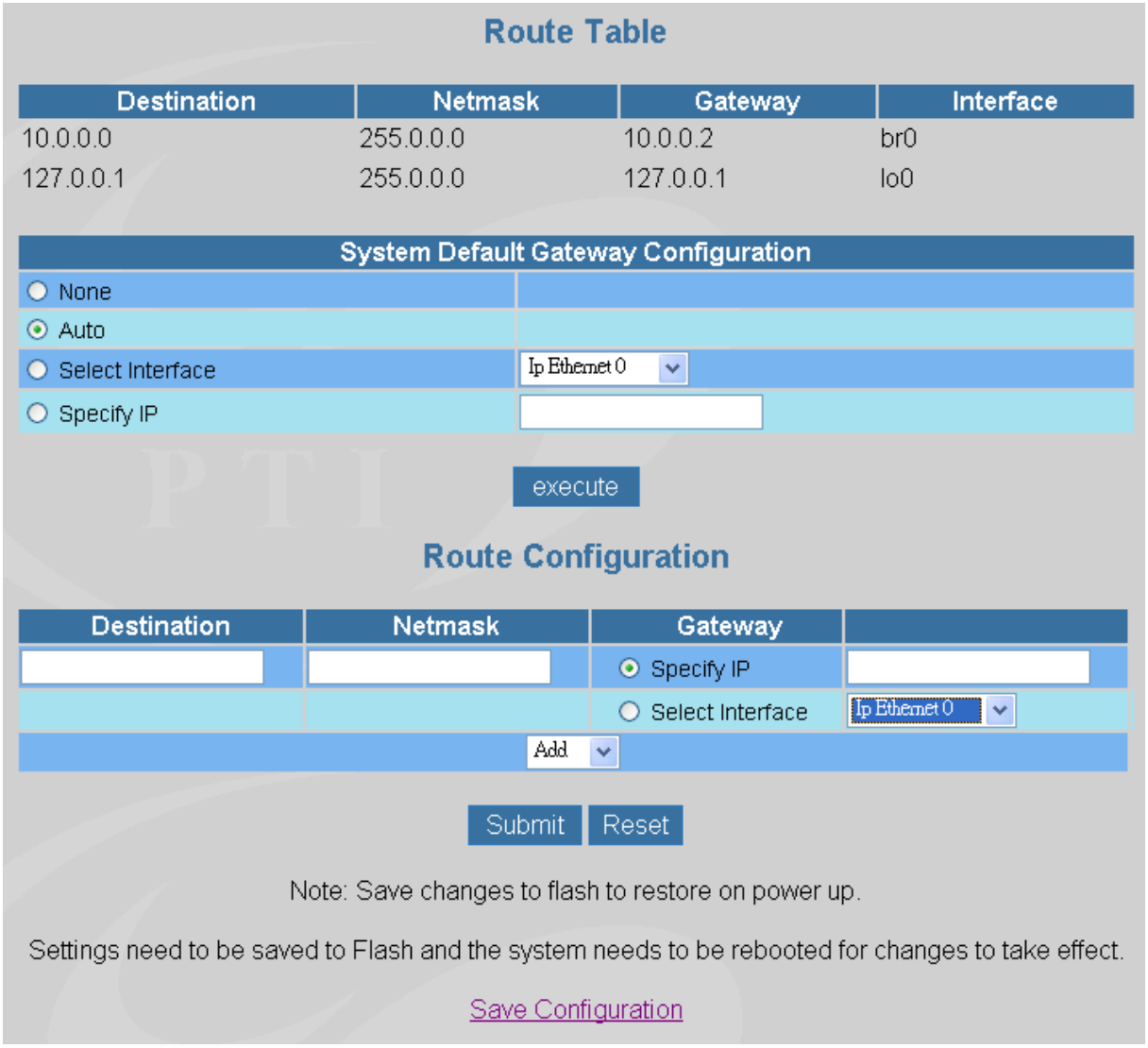
The **ADSL Configuration** page allows you to set the configuration for ADSL protocols.



- Annex Mode Config : This allows you to manually configure the ADSL Router for Annex A or Annex B mode by selecting User Configured and choosing the Annex Mode in the next field.
- User Selected Annex Mode : This allows you to select from Annex A and Annex B.
- Trellis : Trellis Code is an advanced method of FEC (Forward Error Correction). This field allows you to enable or disable the Trellis Code. By default, it is always enabled.
- Handshake Protocol: This field allows you to select from the following ADSL handshake protocols : Autosense – G.dmt first (default), Autosense – T1.413 first, G.dmt/G.lite, T1.413, G.dmt, and G.lite.
- Wiring Selection : This field allows you to enter the wiring selection for the RJ-11. Tip/Ring is the default for the ADSL Router without the inner/outer pair relay. Available types are Auto, Tip/Ring (default), and A/A1, where Tip/Ring is the inner-most pair of wires on the RJ11 and A/A1 is the second inner-most pair.
- Bit Swapping : This field allows you to enable or disable the upstream bit swapping. Bit Swapping is disabled by default.

4.3.3.4 Admin Privilege – Route Table

The **Route Table** page displays the routing table and allows you to manually enter a routing entry. The routing table will display the routing status of Destination, Netmask, Gateway, and Interface. The interface br0 indicates the USB interface; lo0 indicates the loopback interface; ppp1 indicates the PPP interface. The Gateway is the learned Gateway.



- The Gateway field of the static route entry allows users to either enter a Gateway IP address or select a Network Interface.
- All user-defined routes retained in the CPE memory, regardless if they are already in the Routing Table, are displayed on the same Route Table page.
- All user defined route entries kept in the CPE memory during run time are saved to flash when the user chooses to save and reboot the CPE. When the CPE restarts, it reloads all saved user-defined routes to the CPE memory and tries to apply to the system.

- A user-defined route entry is added to the Routing Table whenever the system provides an environment that makes the route entry applicable. It is removed from the Routing Table whenever the route entry becomes not applicable. e.g. If the route entry's Gateway is associated with a dynamic Network Interface but the connection is not established, then the route entry does not appear in the Routing Table. When that interface comes up later, the route entry is then added.

- If the selected Network Interface is static or dynamic and the connection is already up, then the route entry appears in the Routing Table immediately. If there is a Gateway associated with the selected Network Interface, then that Gateway's IP address appears in the Gateway field of the route entry.

  If the selected Network Interface is dynamic but the connection is not established, then the route entry does not appear in the Routing Table. When the interface comes up later, the route entry is then added.

I. System Default Gateway Configuration

The system-wide Default Gateway provides three options: Auto (default), User-selected Network Interface, and None.

- None : This field allows you to choose to have no Default Gateway in the CPE.

- Auto : This field allows you to enable the Bridge/Router to automatically decide the Default Gateway.

- User-selected Network Interface : This field allows you to select a Network Interface from a list (PVCs, PPP Sessions, USB and LAN). This option allows you to associate the system-wide Default Gateway to a Network Interface, static or dynamic, and provides a way to fix the Default Gateway to a dynamic Network Interface before the interface is established.

  Note : The options for this field are IP PVC0 ... IP PVC7, IP Ethernet 0, IP BridgeMux0, and any PPP session that was created by the user.

- Specify IP : This field allows you to specify the IP address of the default gateway.

II. Route Configuration

- Destination : This field allows you to enter the remote network or host IP address for the static routing.

- Netmask : This field allows you to enter the Subnet Mask for the static routing.

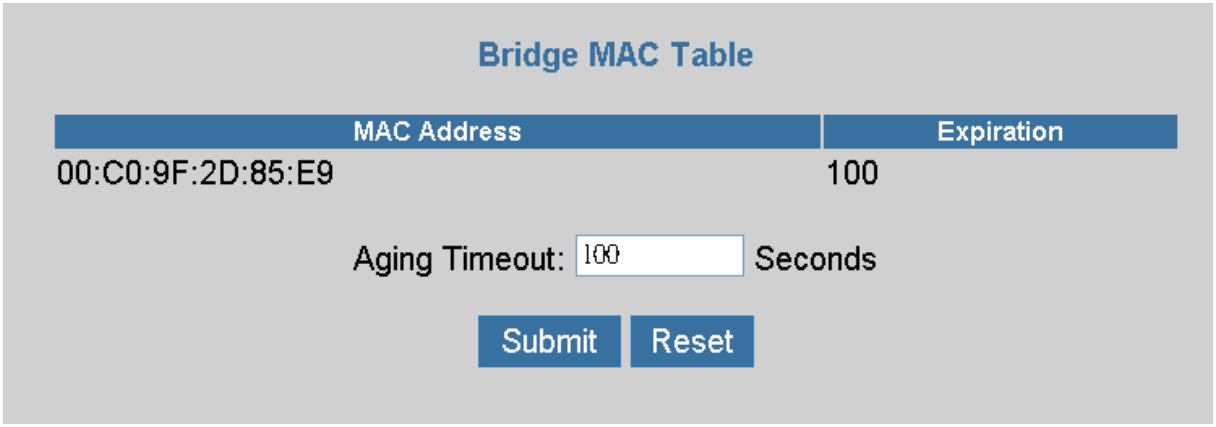
- Gateway : This field allows you to enter the IP address of the gateway device that allows the router to contact the remote network or the host for Specified IP or select an Interface for the Gateway.

- Manually Configured Routes: This field displays the static route entries entered by the user.

4.3.3.5 Admin Privilege – Learned MAC Table

Network bridges operate at the physical network layer. The purpose of a bridge is to connect two or more networks and enable packet sharing between them. Bridges are different from routers because they forward packets based on physical addresses, whereas routers use IP address to forward packets. Bridges must learn all the physical (MAC) addresses of the devices so it can forward the packets reliably. The purpose of the **Learned MAC Table** is to store and display these bridge-recognized MAC addresses.

The **Learned MAC Table** page shows the current learned Bridge MAC table. This page contains information that is dynamic and will refresh every 8 seconds.



- Aging Timeout: This field allows you to enter the update period for the MAC table. Have this number lower if you want a more frequent refresh rate.

  Note :Range for Aging Timeout field is 0 – 32767, default is 100.

4.3.3.6 Admin Privilege – RIP Configuration

RIP (Routing Information Protocol) is a management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge. There are several components to RIP, including the authenticator, supplier, and listener.

Authenticator: Authentication is only available for RIPv2. When it is disabled, RIPv2 messages containing authentication entries are discarded. When it is enabled, all RIPv2 messages must have proper authentication entries, and all RIPv2 messages without verified authentication entries and all RIPv1 messages are automatically rejected.

Supplier: The RIP Supplier has two functions:

I. It transmits route updates over every RIP Supplier interface at the interval specified by **Supply Interval** (see below).

II. It transmits route updates in response to specific requests from other routers.

Listener: The RIP Listener listens and processes all RIP messages it receives from other RIP routers and updates the host routing tables accordingly. The RIP Listener is always enabled when RIP is enabled. By default, RIP is disabled.

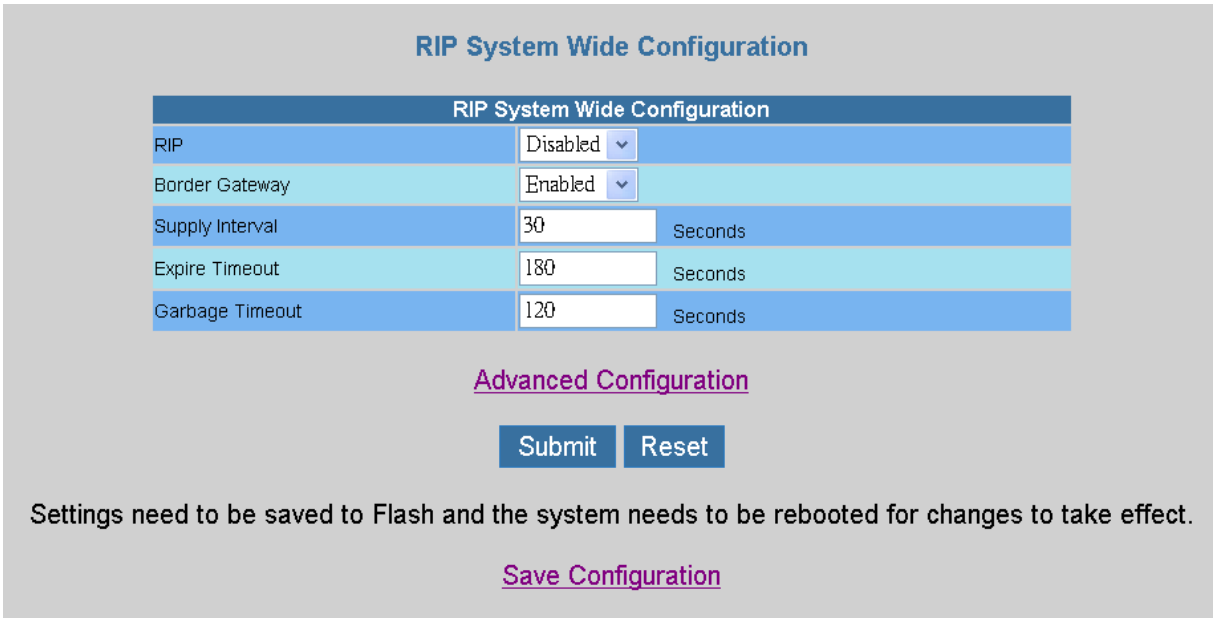
The announcement messages RIP sends are based on two configuration parameters: RIP Version number and Multicast:

Version	Multicast	Announcements Sent
1	OFF	V1
2	ON	V1
2	OFF	V2-BC
2	ON	V2-MC

The RIP messages that can be received and processed are based on two configuration parameters: RIP Version number and Multicast:

Version	Multicast	RIP Messages Received
1	OFF	V1
2	ON	V1
2	OFF	V1 & V2-BC
2	ON	V2-BC & VC-MC

The **RIP Configuration** page allows you to set the configuration for the system wide configuration of RIP. The actual RIP configuration is in the RIP Per Interface Configuration.



- RIP: This field allows you to Enable or Disable the RIP session. The resulting RIP session will monitor all network interfaces that are currently available for messages from other RIP routers. RIP is disabled by default.

- Border Gateway: RIP implements Border Gateway as specified in RFC 1058 and RFC 1723. This limits all subnet routes and host routes to routers within that same network. Updates sent outside that network will only include a single entry representing the entire network, including all subnets and host-specific routes. The Border Gateway is enabled by default.

- Supplier Interval: This field allows you to enter the Supplier Interval timer in seconds. This timer specifies how often the RIP sends announcements as a RIP Supplier.

Note : Range for Supplier Interval field is 0 – 2147483647, default value is 30.

- Expire Timeout: This field allows you to enter the Expire Timeout in seconds. This timer specifies the expiration time of a route. When a route has not been updated for more than the "expire" period of time, it is removed from the Route Table. This route is then invalidated and remains in the internal RIP Route Table. It will be included in the RIP announcements to let other routers know the changes.

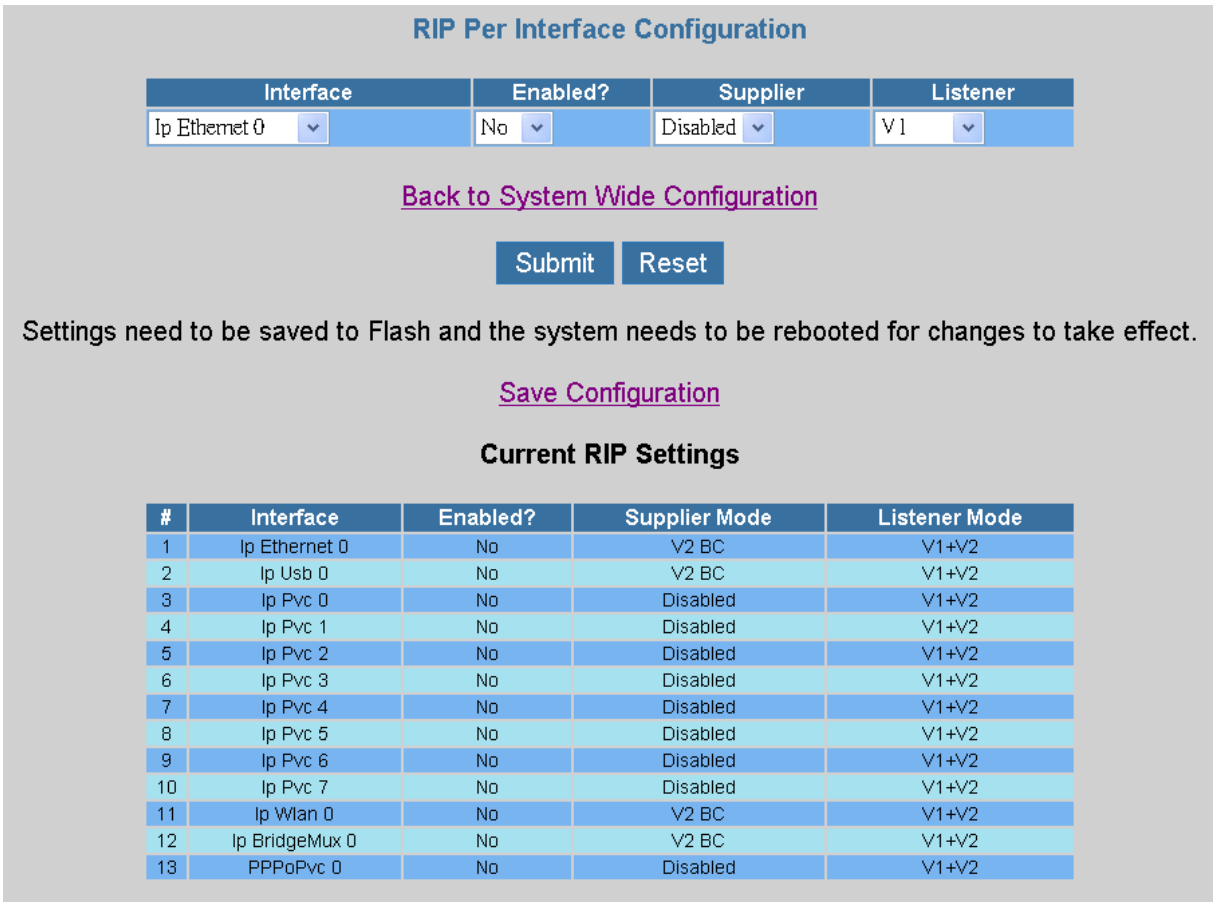
Note : Range for Expire Timeout field is 0 – 2147483647, default is 180.

- Garbage Timeout: This field allows you to enter the Garbage timer in seconds. This timer specifies how long the expired and invalidated routes are kept in the Internal RIP Route Table before they are removed from it.

Note : Range for Garbage Timeout field is 0 – 2147483647, default is 120.

I. Advance Configuration :

The RIP Per Interface Configuration page allows you to set the configuration for each Interface (PVCs, PPP Sessions, USB and LAN).



RIP Per Interface Configuration

Interface	Enabled?	Supplier	Listener
Ip Ethernet 0	No	Disabled	V1

Back to System Wide Configuration

Submit Reset

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

Save Configuration

Current RIP Settings

#	Interface	Enabled?	Supplier Mode	Listener Mode
1	Ip Ethernet 0	No	V2 BC	V1+V2
2	Ip Usb 0	No	V2 BC	V1+V2
3	Ip Pvc 0	No	Disabled	V1+V2
4	Ip Pvc 1	No	Disabled	V1+V2
5	Ip Pvc 2	No	Disabled	V1+V2
6	Ip Pvc 3	No	Disabled	V1+V2
7	Ip Pvc 4	No	Disabled	V1+V2
8	Ip Pvc 5	No	Disabled	V1+V2
9	Ip Pvc 6	No	Disabled	V1+V2
10	Ip Pvc 7	No	Disabled	V1+V2
11	Ip Wlan 0	No	V2 BC	V1+V2
12	Ip BridgeMux 0	No	V2 BC	V1+V2
13	PPPoPvc 0	No	Disabled	V1+V2

- Interface: This field allows you to choose the Interface (PVCs, PPP Sessions, USB and LAN), for the RIP to be configured. The available selections are: IP Ethernet 0, IP USB 0, IP PVC0...IP PVC7, IP BridgeMux 0, and any PPP user defined sessions (maximum of 16)

- Enable: This field allows you to Enable (Yes) or Disable (No) the specified interface for RIP.

- Supplier: This field allows you to select the Supplier Mode (RIP Transmit).

    1. Disabled: The supplier transmit is disabled.
    2. V1 BC: The supplier transmits in RIPv1 Broadcast.
    3. V2 BC: The supplier transmits in RIPv2 Broadcast.
    4. V2 MC: The supplier transmits in RIPv2 Multicast.

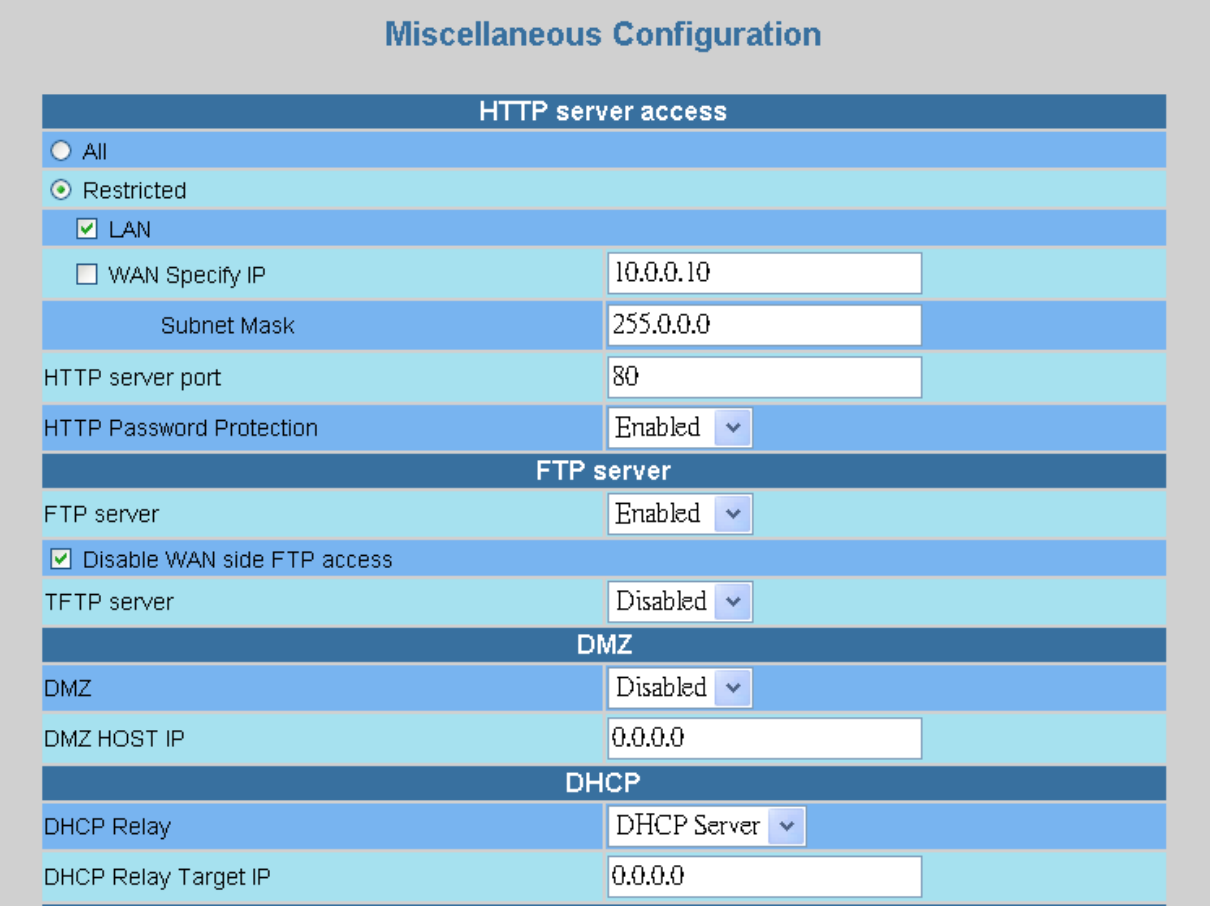
- Listener: This field allows you to select the Listener Mode (RIP Receive)

    1. V1: The listener receives the RIPv1 only.
    2. V2: The listener receives the RIPv2 only.
    3. V1+V2: This listener receives the both RIPv1 and RIPv2.

- Current RIP Settings: This field displays the each interface's RIP status.

4.3.3.7 Admin Privilege – Misc Configuration

The **Miscellaneous Configuration** page allows you to set miscellaneous configurations for the following: HTTP, FTP, TFTP, DMZ, Command Line Interface, DHCP, PPP, IGMP, and SNTP.



I. HTTP Server Access :

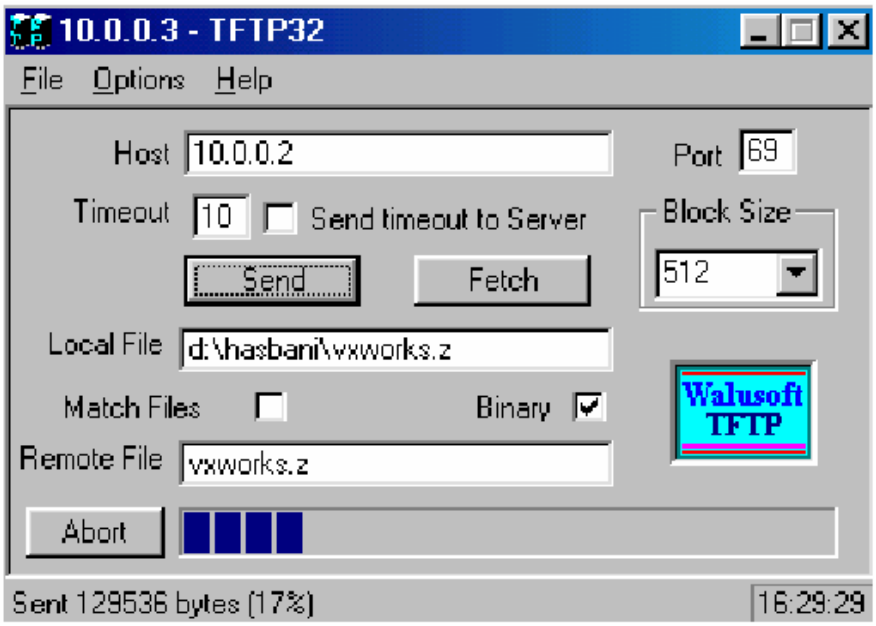
This field allows you to configure where these Web pages can be accessed from.

- **All:** When this field is checked, it allows both WAN and LAN access to the Web pages. This is the system default.
- **Restricted LAN:** This field allows the Web pages access from LAN side.
- **Restricted WAN Specified IP & Subnet Mask:** This field allows the Web access from WAN side with a specify IP and subnet mask.
- **HTTP Server Port:** This field allows you to specify the port of the Web access. . For example, when it is changed to 8080, the HTTP server address for the LAN side is http://10.0.0.2:8080. Range for HTTP Server port is 0 – 32767, default value is 80.

II. FTP Server :

- **FTP server:** This field allows you to enable or disable the FTP server connection. System default is Enabled.
- **Disable WAN side FTP access:** This will disable WAN side access to the FTP server, default is Disabled.
- **TFTP server:** This field allows you to enable or disable the TFTP connection. System default is Disabled.

An example for the TFTP client updating the vxworks.z product image code is:

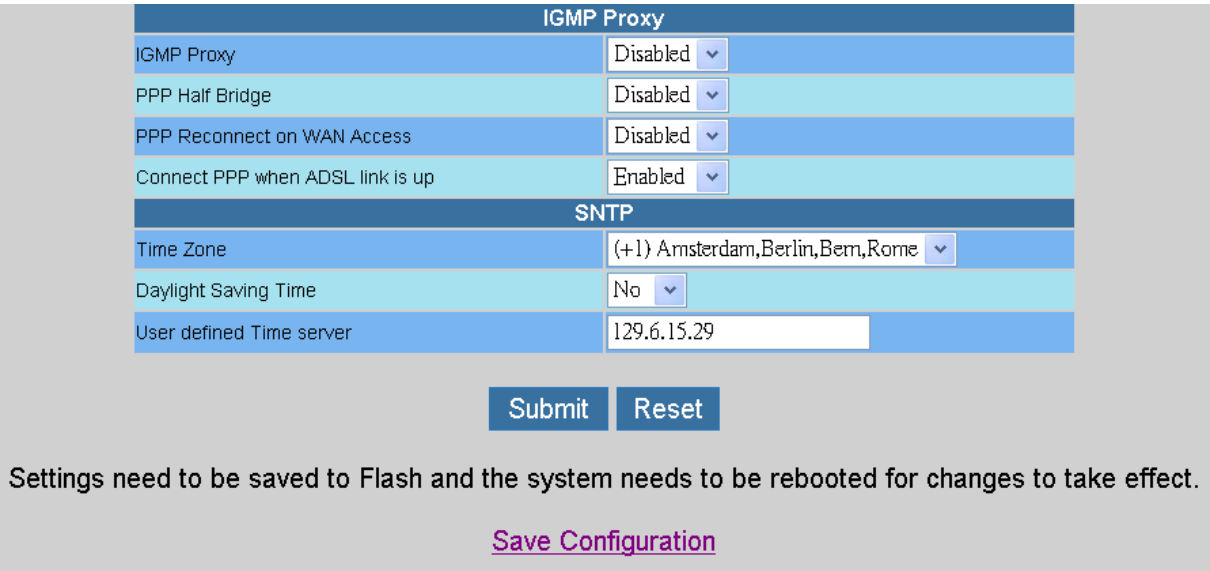


III. DMZ :

- **DMZ:** A DMZ (De-Militarized Zone) is added between a protected network and an external network, in order to provide an additional layer of security. When there is a suspected packet coming from WAN, the firewall will forward this packet to the DMZ host.
- **DMZ Host IP:** The IP address of the DMZ host viewable at the WAN (external) side.

IV. DHCP :

- DHCP Relay :
  - **NONE:** This will disable the DHCP server. Note that this setting will override the DHCP Server Enable/Disable on the LAN configuration page.
  - **DHCP Server** (default)**:** Select this to activate the DHCP server.
  - **DHCP Relay:** If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please disable the NAT to run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.
- **DHCP Relay Target IP:** If DHCP Relay is enabled, DHCP requests are relayed to DHCP Target IP on the WAN side.



V. IGMP Proxy :

- **IGMP Proxy:** This is the global setting for IGMP Proxy. If it is enabled, then the enabled IGMP Proxy on WAN PVCs will be working. Otherwise, no WAN PVC can have IGMP Proxy working on it. System default is Disabled.
- **PPP Half Bridge:** When PPP Half Bridge is enabled, only one PC is able to access the Internet, and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet. System default is Disabled.
- **PPP reconnect on WAN access:** If enabled, the PPP session will automatically establish a connection when a packet tries to access the WAN. System default is Disabled.

- **Connect PPP when ADSL link is up:** If this option is enabled, the bridge/router will connect the PPP session whenever an ADSL connection is established. If this option is disabled, the PPP session will not connect whenever the ADSL Showtime is reached. System default is Enabled.

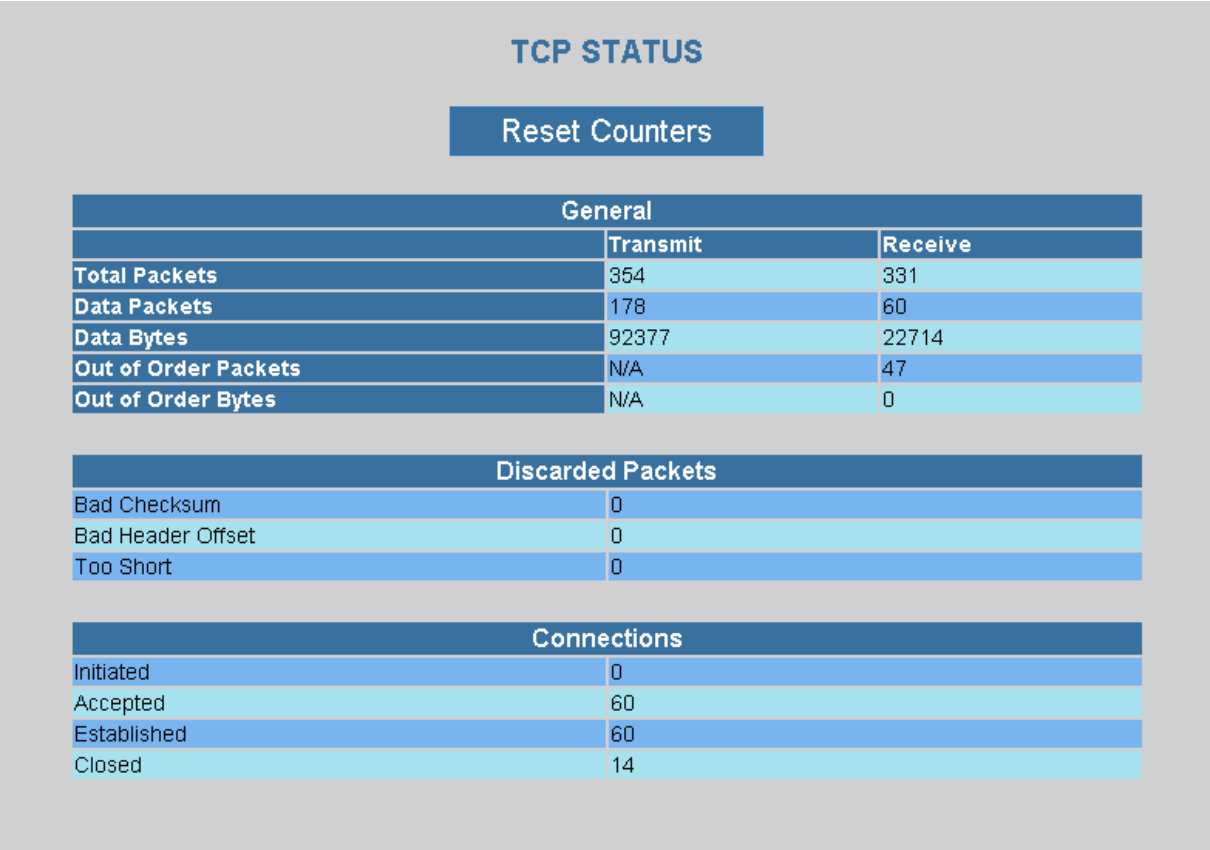
Note: For more information/clarification, please refer to PPP Configuration section.

VI. SNTP :

- **SNTP:** Simple Network Time Protocol is a efficient method of obtaining the time from a Time Server.
- **Time Zone:** This specifies the time zone (geographical location).
- **Daylight Saving Time:** You can select yes to activate Daylight Savings Time.
- **User defined Time server:** This is the time server from which the ADSL Router retrieves the time.

4.3.3.8 Admin Privilege – TCP Status

The **TCP Status** page shows the statistics for all TCP connections. This page contains information that is dynamic and will refresh every 2 seconds.



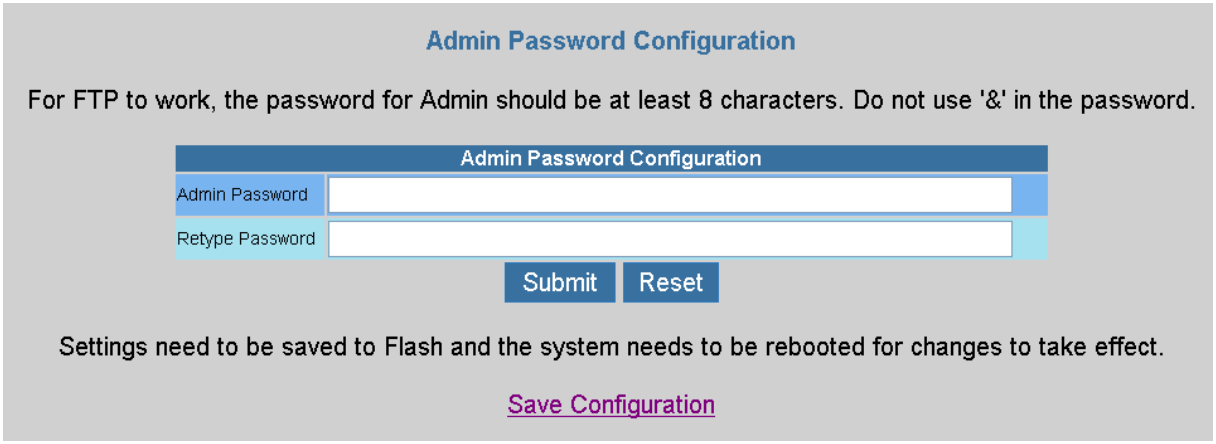
- Reset Counters: This button allows user to reset the TCP Status counter.
- General: Total Packets, Data Packets, Data Bytes, Out of Order Packets, Out of Order Bytes.
- Discarded Packets: Bad Checksum, Bad Offset Header, Too Short.
- Connections: Initiated, Accepted, Established, Closed.

4.3.3.9 Admin Privilege – Admin Password Configuration

The **Admin Password Configuration** page allows you to set the password for administrator.

The Admin password is same as the FTP password, so it must have at least 8-characters for the FTP to work.

The Admin password can be up to 65 characters (excluding ‘&’).

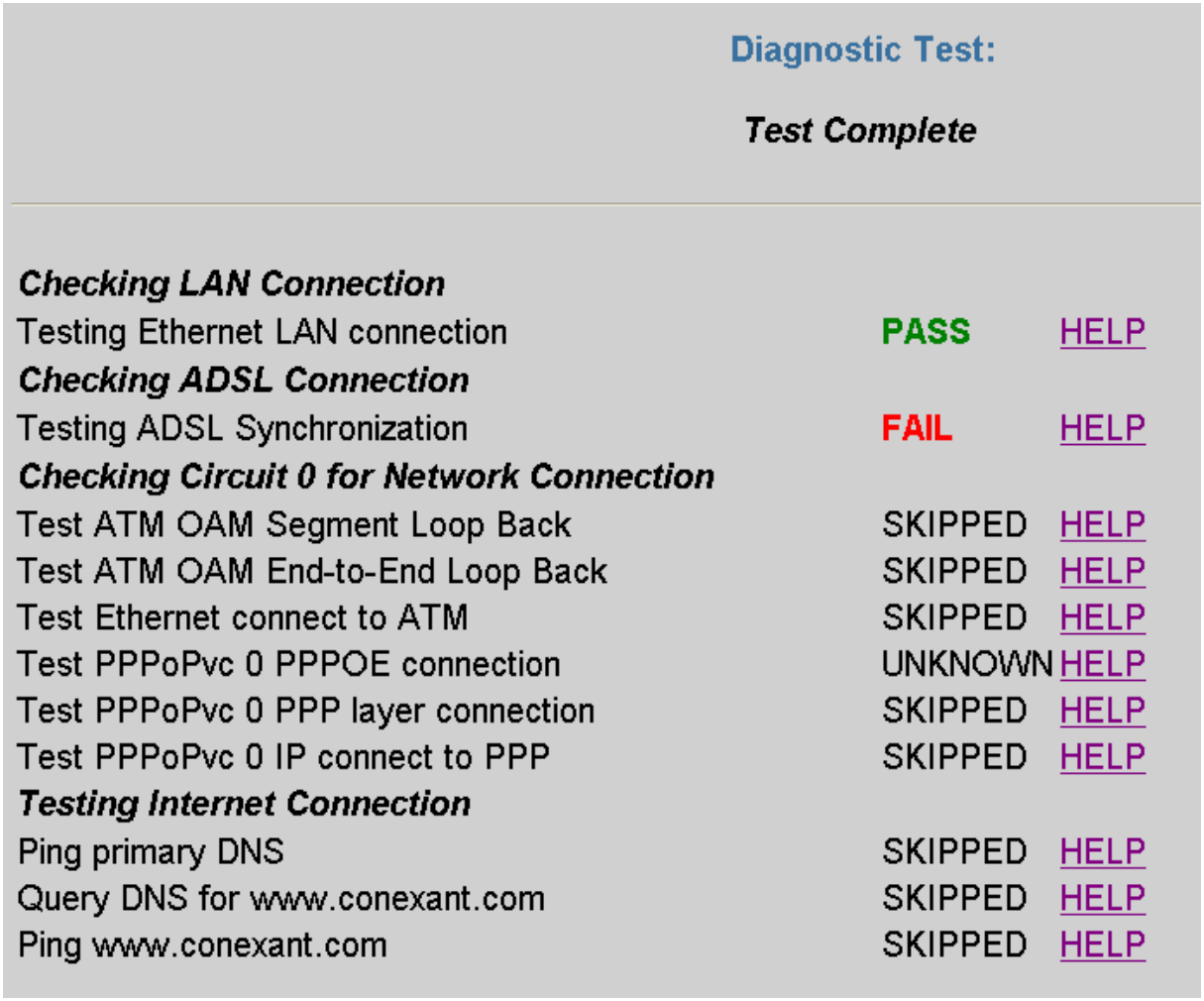

Admin Password Configuration
For FTP to work, the password for Admin should be at least 8 characters. Do not use '&' in the password.
Admin Password Configuration
Admin Password
Retype Password
Submit
Reset
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

4.3.3.10 Admin Privilege – Reset To Factory Default

The **Reset to Factory Default** page allows you to reset the ADSL Router to original factory default configuration (factory.reg).

4.3.3.11 Admin Privilege – Diagnostic Test

The **Diagnostic Test** page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides. This page will continually refresh every 2 seconds until all tests are complete.


Diagnostic Test:
Test Complete
Checking LAN Connection
Testing Ethernet LAN connection PASS HELP
Checking ADSL Connection
Testing ADSL Synchronization FAIL HELP
Checking Circuit 0 for Network Connection
Test ATM OAM Segment Loop Back SKIPPED HELP
Test ATM OAM End-to-End Loop Back SKIPPED HELP
Test Ethernet connect to ATM SKIPPED HELP
Test PPPoPvc 0 PPPOE connection UNKNOWN HELP
Test PPPoPvc 0 PPP layer connection SKIPPED HELP
Test PPPoPvc 0 IP connect to PPP SKIPPED HELP
Testing Internet Connection
Ping primary DNS SKIPPED HELP
Query DNS for www.conexant.com SKIPPED HELP
Ping www.conexant.com SKIPPED HELP

I. Checking LAN Connection :

- **Testing Ethernet LAN Connection:** This test passes if the Ethernet LAN interface is working properly.

II. Checking ADSL Connection :

- **Testing ADSL Synchronization:** This test checks your ADSL Router to see if it can successfully negotiate and establish an ADSL connection with your service provider. The test returns PASS if an ADSL connection is established.
  If this test returns FAIL, please try the test again a few minutes after this test is completed. Your ADSL Router needs up to one minute to establish the ADSL connection depending on your phone line quality. If this test returns FAIL, make sure your phone line is connected to your ADSL Router secured, and also check with your service provider to see if your service is activated.

  If this test returns FAIL, all other tests will be skipped.

III. Checking Circuit 0 For Network Connection :

- **Test ATM OAM Segment Loop Back:** This test sends ATM OAM F5 Segment loop back request cells to the CO. This test will pass if a response cell is received. Since some service providers might not support this test, it could still work even if this test fails. If this test fails consistently and the ADSL Router seems not working, make sure the VPI and VCI are configured correctly.
  This test returns FAIL if the ADSL synchronization test failed.

- **Test ATM OAM End-to-End Loop Back:** This test sends ATM OAM F5 End to End loop back request cells to the central office equipment through your ADSL connection. This test returns PASS if response cell is received. Since your service provider might not support this test, your ADSL Router could still be working properly even if this test fails.
  If this test returns FAIL consistently and your ADSL Router seems to not be working, check to make sure the VPI and VCI are configured correctly.

  This test returns SKIPPED if the ADSL synchronization test failed.

- **Test Ethernet Connect to ATM:** This test returns PASS if the ATM AAL5 module is loaded correctly in your ADSL Router. If this test returns FAIL, an internal error has occurred.
  This test returns SKIPPED if the ADSL synchronization does not return PASS.

- **Test PPPoE Connection:** This test returns PASS if your ADSL Router can see the PPPoE server.
  If this test returns FAIL, run this test again a few minutes after this test is completed, especially if your PPPOE connection has just been improperly disconnected.

  If this test consistently returns FAIL, make sure that the PPPoE settings are in the correct configuration as instructed by your service provider, make sure the VPI and the VCI settings

of the current VC are configured correctly.

This test returns SKIPPED if the “AAL5 Connection” test does not return PASS.

- **Test PPP Layer Connection:** This test returns PASS if your login name and password have passed authentication with your service provider.
  If this test returns FAIL, run this test again a few minutes after this test is completed, especially if your PPP connection has just been improperly disconnected. If this test consistently fails, first make sure your login name and password are correct. Remember that login names and passwords are case sensitive.

  This test returns SKIPPED if the “PPPoE Connection” test does not return PASS and your ADSL modem is configured as PPPoE encapsulation.

  This test also returns SKIPPED if the “AAL5 Connection” test does not return PASS and your ADSL Router is configured for PPPOA encapsulation.

- **Test IP Connect to PPP:** This test returns PASS if your ADSL Router has been assigned a valid IP address by your service provider through DHCP or your ADSL Router is assigned a valid IP address statically.

  If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your ADSL Router is statically assigned an IP address, make sure the IP address is the correct one assigned by your service provider.

  This test returns SKIPPED if the “AAL5 Connection” test does not return PASS.

IV. Testing Internet Connection :

- **Ping Gateway:** This test returns PASS if the gateway can be reached through a ping request. The gateway is assigned by your service provider, or obtained from your service provider by PPP or DHCP negotiation.

  If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your ADSL Router seems not working, check to make sure your statically assigned IP address is configured correctly or the DHCP client is enabled on with the current VC.

  This test returns SKIPPED if the “IP Assignment” test does not return PASS.

- **Ping Primary DNS:** This test returns PASS if the primary DNS can be reached through a ping request. The primary DNS is assigned by your service provider or obtained from your service provider by PPP or DHCP negotiation.

  If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your ADSL Router seems to not be working, check to make sure your statically assigned primary DNS IP address is configured correctly or DHCP client is enabled with the current VC.

  This test returns N/A if there is no DNS configured.

- **Query DNS for www.conexant.com:** This test returns PASS if the host name can be resolved to an IP address though your domain name servers. This test returns FAIL if the host name can not be resolved successfully.

  If this test returns FAIL, run this test again a few minutes after this test is completed.

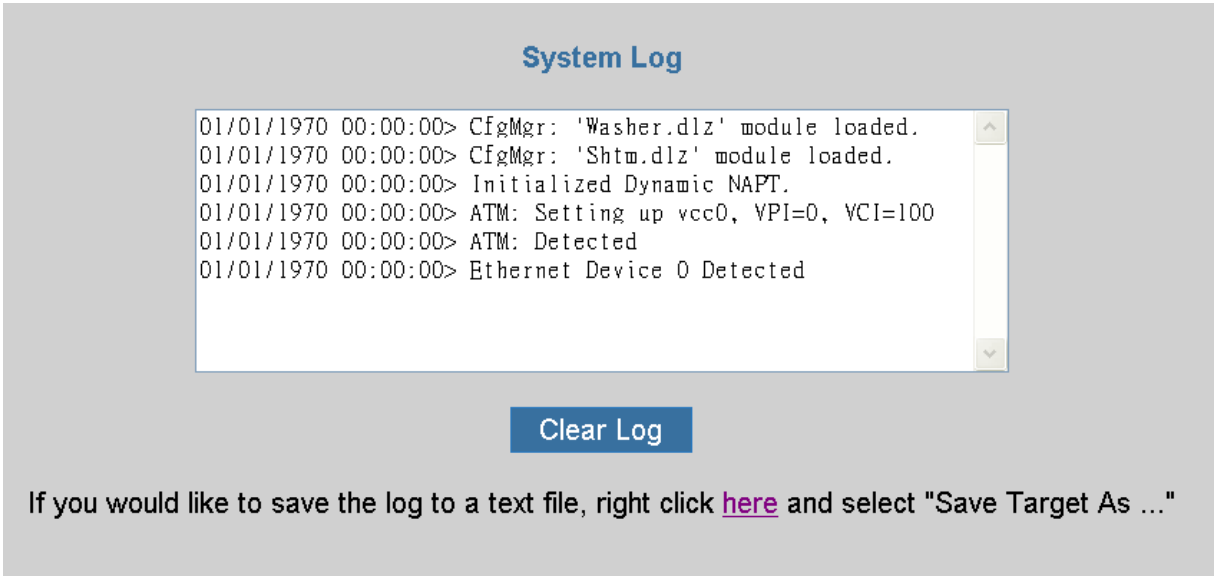
- **Ping www.conexant.com:** This test returns PASS if the host specified by your ISP can be reached through a ping request.

  If this test returns FAIL, run this test again a few minutes after this test is completed.

  This test returns SKIPPED if the host name can not be resolved to an IP address.

4.3.3.12 Admin Privilege – System Log

The **System Log** page shows the events triggered by the system. This page contains information that is dynamic and will refresh every 5 seconds.

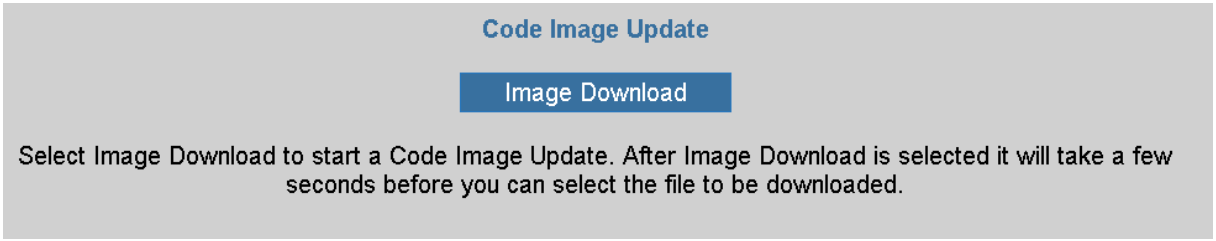

System Log
01/01/1970 00:00:00> CfgMgr: 'Washer.dlz' module loaded.
01/01/1970 00:00:00> CfgMgr: 'Shtm.dlz' module loaded.
01/01/1970 00:00:00> Initialized Dynamic NAPT.
01/01/1970 00:00:00> ATM: Setting up vcc0, VPI=0, VCI=100
01/01/1970 00:00:00> ATM: Detected
01/01/1970 00:00:00> Ethernet Device 0 Detected
Clear Log
If you would like to save the log to a text file, right click here and select "Save Target As ..."

- Clear Log: This field allows you to clear the current contents of the System Log.
- Save Log: This field allows you to save the current contents of the System Log by right click **"HERE"** and select **"Save Target As"** to save it into a text file.
- The System Log records:
  - ADSL Layer :
    - ADSL Link detected
    - ADSL Link connected
    - ADSL Link disconnected
  - ATM Layer :
    - ATM detected
    - ATM connected
    - ATM disconnected
    - ATM setting up VPI/VCI
  - PPP Layer :
    - PPP authenticated
    - PPP invalid user name or password
    - PPP unable to connect with PPP server
  - IP Layer :
    - IP protocol up
    - PPP IP address
    - PPP Gateway IP address PPP DNS Primary IP address
    - PPP DSN Secondary IP address

4.3.3.13 Admin Privilege – Local Code Image Update

The **Code Image Update** page allows you to upgrade the image code locally.

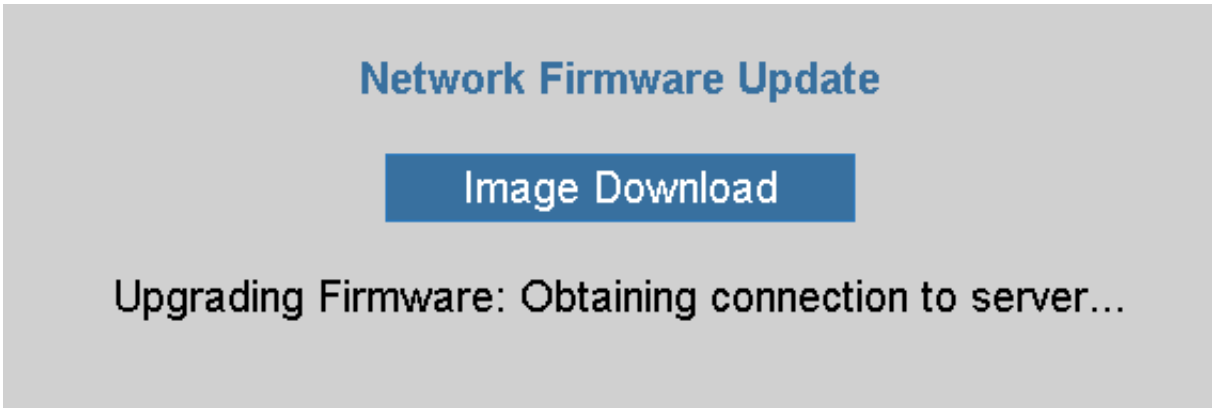
Browse the location of file, firmware.dlf or bootrom.dlf file, and click the Upload to start the update. The ADSL Router will reboot as part of the process of updating code.


Code Image Update
Image Download
Select Image Download to start a Code Image Update. After Image Download is selected it will take a few seconds before you can select the file to be downloaded.

4.3.3.14 Admin Privilege – Network Firmware Image Update

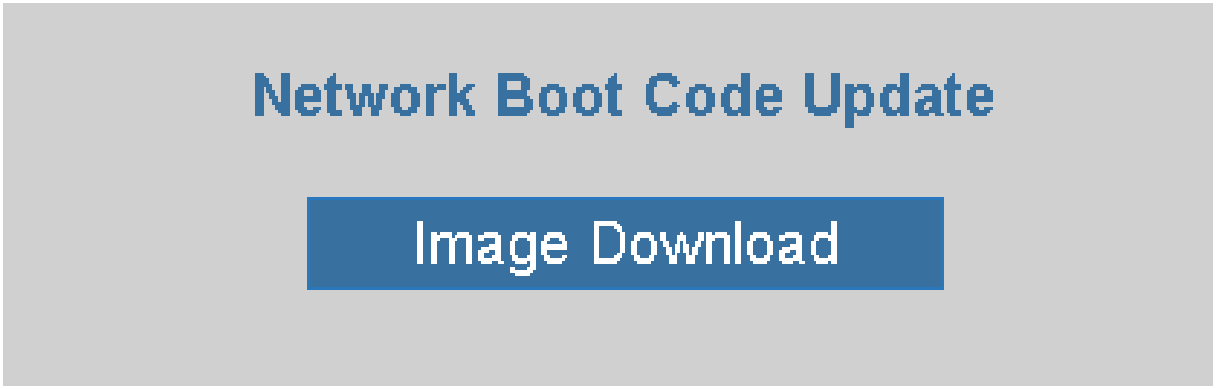
The **Network Firmware Image Update** page allows you to upgrade the image code from the remote FTP server.

Assume an FTP server stores the updated image firmware.dlf on Internet. Click Image Download to initiate the updating. The ADSL Router will reboot as part of the process of updating code.

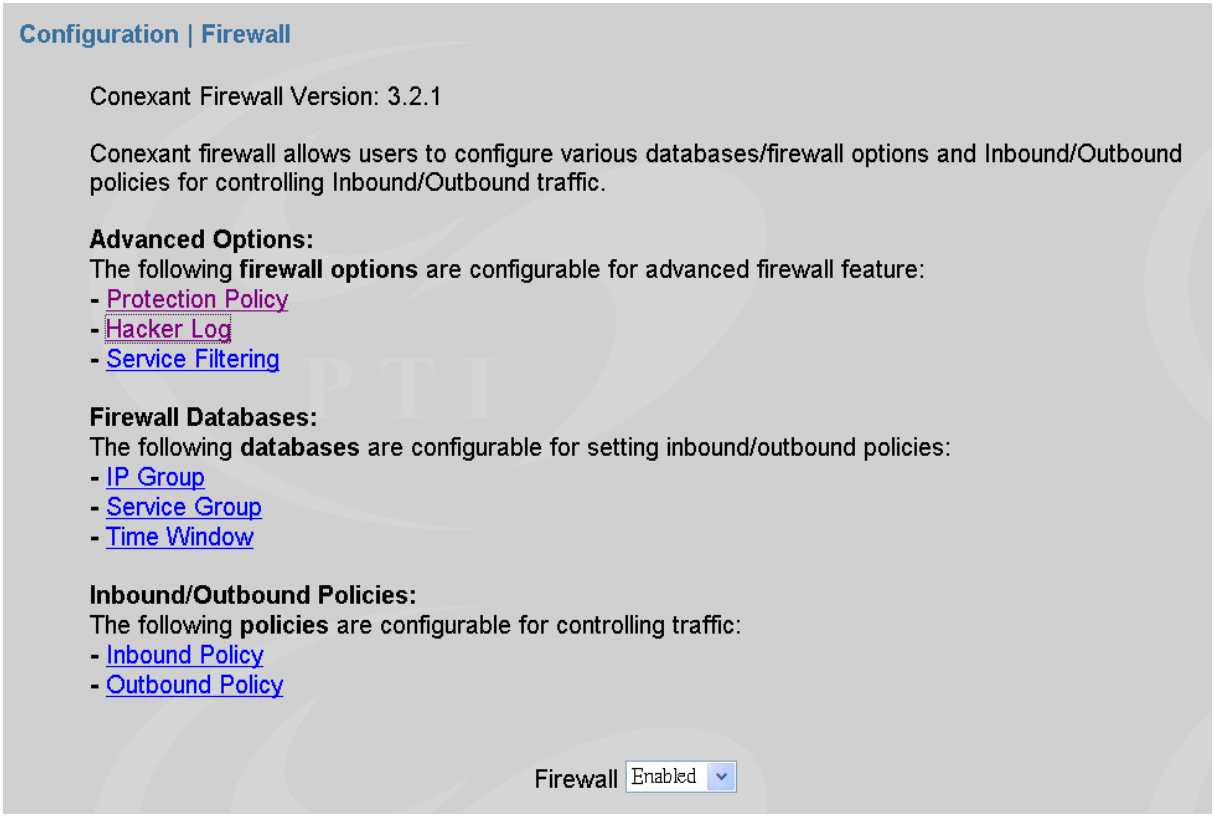


4.3.3.15 Admin Privilege – Boot Code Image Update

Assume an FTP server stores the updated image boorom.dlf on Internet. Click Image Download to initiate the updating. The ADSL Router will reboot as part of the process of updating code.



4.3.3.16 Admin Privilege – Firewall


Configuration | Firewall
Conexant Firewall Version: 3.2.1
Conexant firewall allows users to configure various databases/firewall options and Inbound/Outbound policies for controlling Inbound/Outbound traffic.
Advanced Options:
The following firewall options are configurable for advanced firewall feature:
- Protection Policy
- Hacker Log
- Service Filtering
Firewall Databases:
The following databases are configurable for setting inbound/outbound policies:
- IP Group
- Service Group
- Time Window
Inbound/Outbound Policies:
The following policies are configurable for controlling traffic:
- Inbound Policy
- Outbound Policy
Firewall
Enabled

Note : A Statefull Packet Inspection (SPI) firewall is an optional feature that may or may not be included in your ADSL Router.

A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Advanced Options: This section contains options for protecting against particular well known attacks as well as documenting those attacks as they occur.

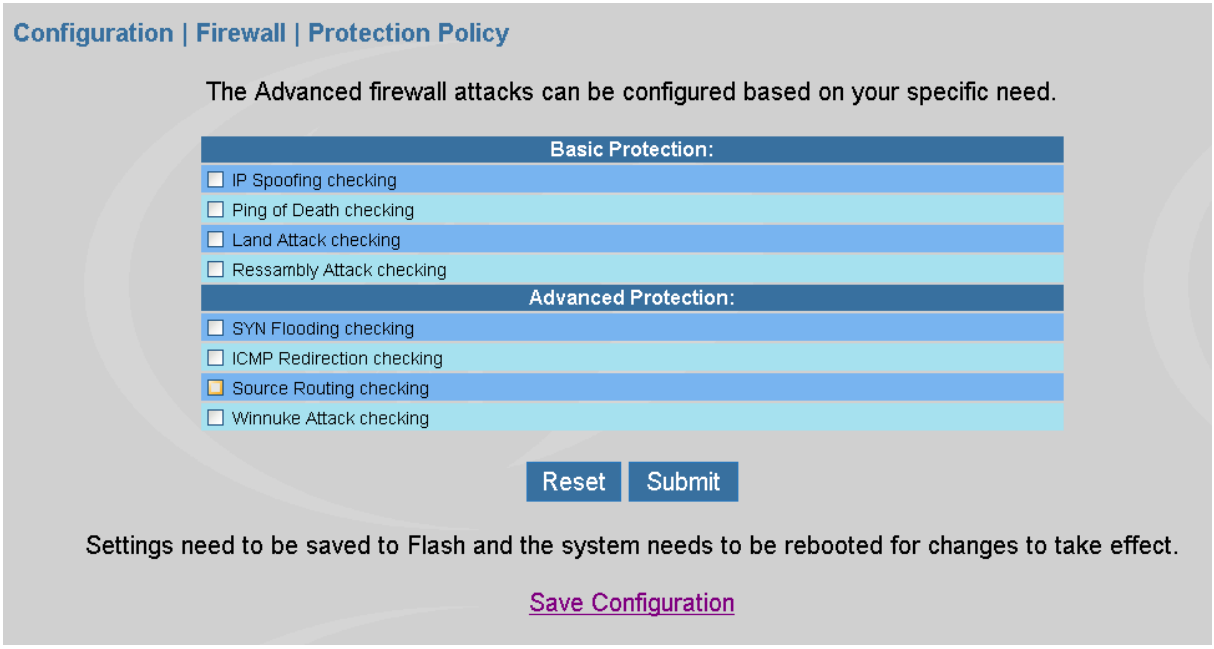
Firewall Databases: This section allows you to create groups based on IP addresses, subnet masks, ports, and time. These groups are used when creating inbound and outbound policies.

Inbound/Outbound Policies: This section allows you to create rules for incoming and outgoing IP packets. The IP packets are compared against the rules and are allowed or denied accordingly.

Firewall Enable/Disable: This option enables/disables all the protection provided on these pages.

4.3.3.16.1.1 Advanced Options – Protection Policy

Protection Policies defend against common methods of attacking a network and computers within the network. Some of these attacks are classified as a DoS (Denial of Service). DoS is an attack in which a network or components of a network are disabled, usually by overloading traffic on the network, in order to prevent authorized and legitimate users to access network resources.


Configuration | Firewall | Protection Policy
The Advanced firewall attacks can be configured based on your specific need.
Basic Protection:
IP Spoofing checking
Ping of Death checking
Land Attack checking
Ressambly Attack checking
Advanced Protection:
SYN Flooding checking
ICMP Redirection checking
Source Routing checking
Winnuke Attack checking
Reset
Submit
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

- Basic Protection:
  - **IP Spoofing checking:** IP spoofing is when an unauthorized user inserts the IP address of an authorized user into the IP packets in order to gain access to a network. Selecting this option will allow the firewall to check for and filter out this discrepancy.
  - **Ping of Death checking:** Ping of Death is a type of DoS attack that uses a malformed ICMP data packet that contains unusually large amounts of data that causes TCP/IP to crash or behave irregularly. Enabling this will allow the firewall to filter out packets containing Ping of Death properties.
  - **Land Attack checking:** Land attack is a type of DoS attack that works by sending a spoofed packet containing the same source and destination IP address and port (the victim's IP address). This packet contains a connection request, resulting in a handshake process. At the end of the handshake, the victim sends out an ACK (ACKnowledge) request. Since the source and the destination are the same, the victim receives the ACK request it just sent out. The received data does not match what the victim is expecting, so it retransmits the ACK request. This process repeats until the network crashes. Enabling this will allow the firewall to filter out possible Land Attack packets.

- **Reassembly Attack checking:** Reassembly Attack is a type of DoS attack that exploits the weakness of the IP protocol reassembly process. As discussed earlier in this user guide, packets undergo fragmentation when they exceed a certain maximum size. Certain criteria define the packet fragmentation process so that packets can be reassembled properly. In Reassembly Attack, the subpackets have malformed criteria (fragment offset), which can easily cause a system to crash, freeze, or reboot. Enable this option to check for and filter out Reassembly Attack packets.

◆ Advanced Protection:

- **SYN Flooding checking:** SYN Flooding is a type of DoS attack that is accomplished by not sending the final acknowledgement to the receiving server's SYN-ACK (SYNchronize-ACKnowledge) in the final part of the handshake process. This causes the serve to keep signaling until it is timed out. When a flood (many) of these attacks are sent simultaneously, the server will probably overload and crash. Enable SYN Flooding checking to filter out possible SYN flood packets.

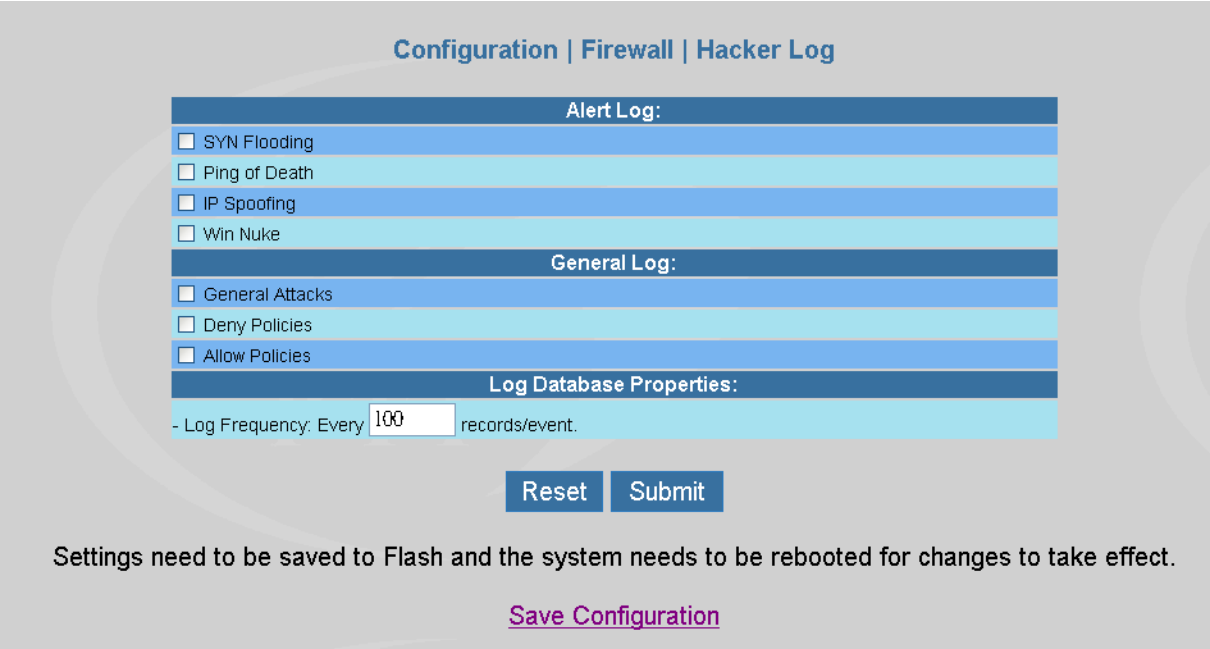
- **ICMP Redirection checking:** Also known as an ICMP storm attack or smurf attack, ICMP Redirection is another form of DoS. This attack is performed by sending ICMP echo requests to a broadcast network node. The return IP address is spoofed and replaced by the victim's own address, causing it to send the request back to itself. This causes the broadcast address to send it out to all the network nodes in the broadcast area (usually the entire LAN). In turn, all those recipients resend it back to the broadcast. The process repeats itself, gaining more amplitude through each iteration and eventually causing a traffic overload and crashing the network. Enable ICMP Redirection checking to filter out packets containing the threat.

- **Source Routing checking:** Source routing gives the sender of a packet the ability to determine the exact route that an IP packet takes to get to the destination. However, source routing can be used for malicious reasons. Using a source routed packet, the sender could find out important information about nodes in a network, making it easy to exploit any weakness. Enabling Source Routing checking will cause the firewall to filter out any packet with Source Routing properties.

- **WinNuke Attack checking:** WinNuke exploits a large networking bug found in Windows 95 and NT. WinNuke sends erroneous OOB (Out-of-Band) data that Windows is unable to process, causing the target computer to crash. Enable this if you are running an early (95 or NT) version of Windows that is vulnerable to this attack.

4.3.3.16.1.2 Advanced Options – Hacker Log

This page allows you to configure which Protection Policy (see previous section) violations to log for admin viewing.

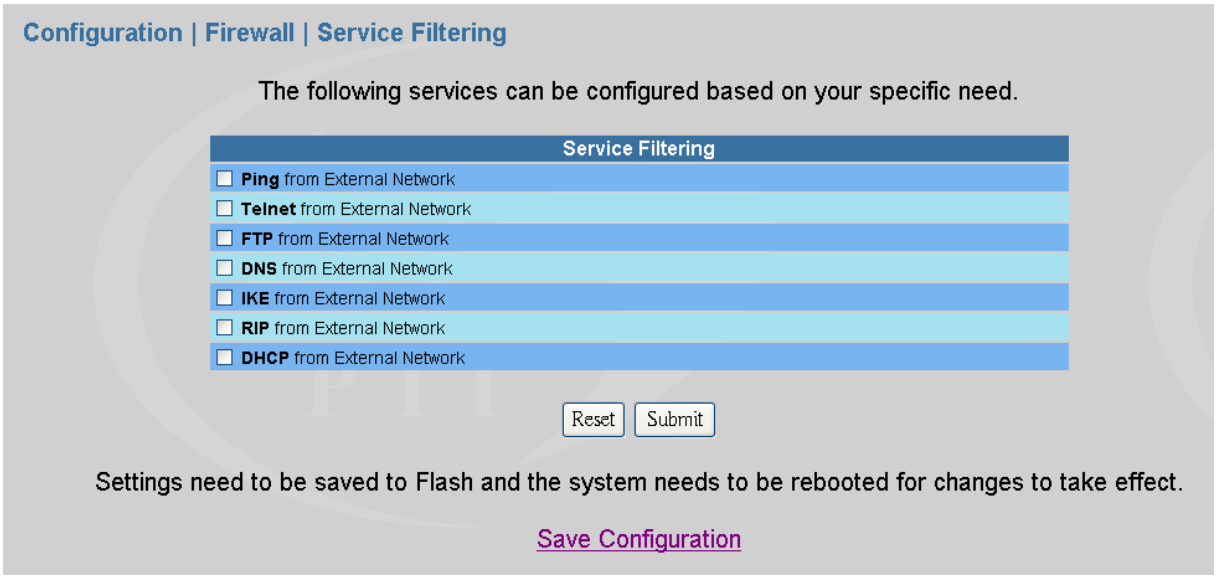


- Alert Log: Enable/Disable for SYN Flooding, Ping of Death, IP Spoofing, and Win Nuke (all of these are explained in the previous section). Enable to log violations of individual policies.
- General Log:
  - Deny Policies: Enabling this will add Deny Policy violations to the log. Deny Policies are discussed later in the Inbound/Outbound policy section.
  - Allow Policies: Enabling this will add Allow Policy acceptances to the log. Allow Policies are discussed later in the Inbound/Outbound policy section.
- Log Database Properties:
  - Log Frequency: This field lets you specify how many records to keep of each event. Default is 100.

    Range for Log Frequency Field is 1-65535.

4.3.3.16.1.3 Advanced Options – Service Filtering

Service Filtering allows you to disable service requests from certain sources.

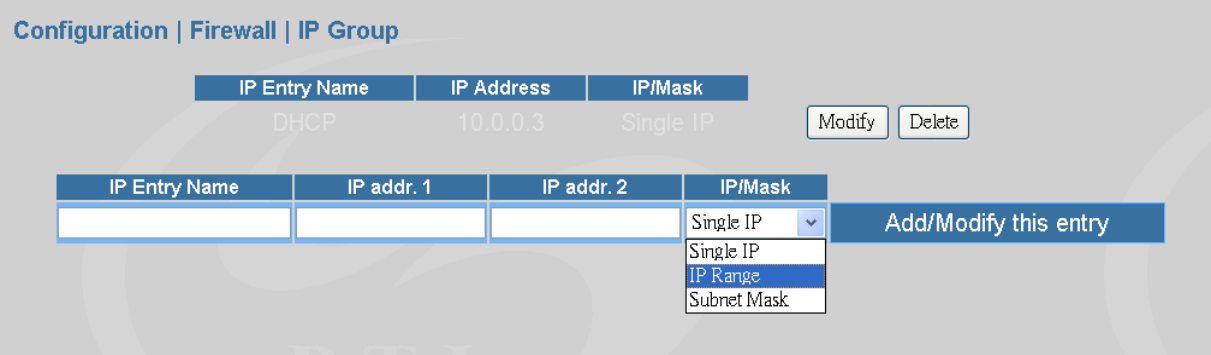

Configuration | Firewall | Service Filtering
The following services can be configured based on your specific need.
Service Filtering
Ping from External Network
Telnet from External Network
FTP from External Network
DNS from External Network
IKE from External Network
RIP from External Network
DHCP from External Network
Reset
Submit
Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
Save Configuration

These are the Service Request sources that can be disabled :

- Ping from External Network
- Telnet from External Network
- FTP from External Network
- DNS from External Network
- IKE from External Network
- RIP from External Network
- DHCP from External Network

4.3.3.16.2.1 Firewall Databases – IP Group

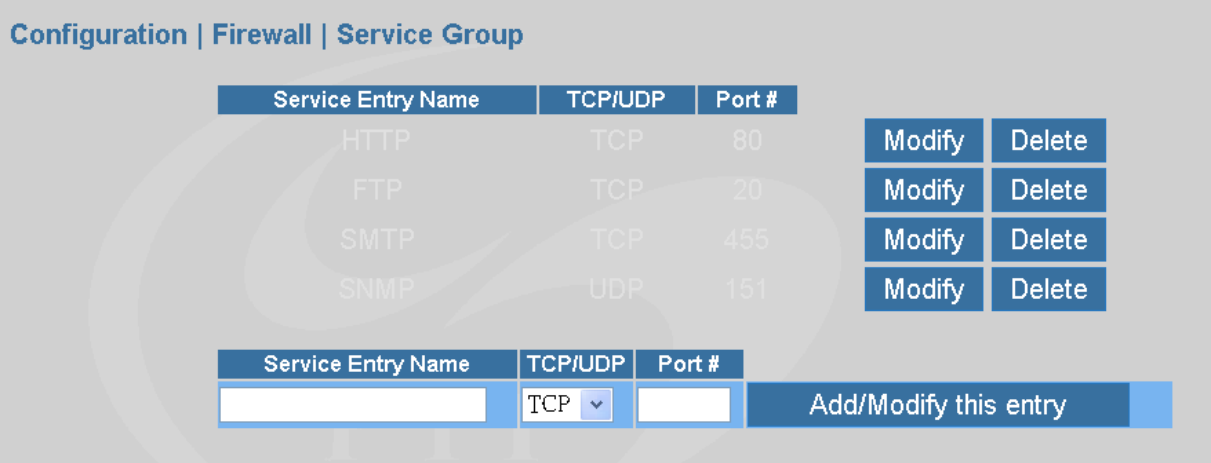
The IP Group lets you specify IP Addresses (Single or Range) and Subnet Masks and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.



- IP Entry Name: This is the name you assign to the group of IP addresses and subnet masks. The IP Entry Name can be up to 19 characters.
- IP addr. 1: This is the IP address or subnet mask you are specifying when creating a group.
- IP addr. 2: This field is only active if you select to group a range of IP addresses or subnet masks, in which case this is the end address of that range whereas the IP addr 1 is the first address of that range.
- IP/Mask: This field allows you to specify the address type assigned to the group.
    - Single IP: This will let you specify one IP address for a given group.
    - IP Range: This will let you specify a range of IP addresses for a given group, starting with IP addr 1 and ending with IP addr 2.
    - Subnet Mask: This will let you specify a range of subnet masks for a given group.

4.3.3.16.2.2 Firewall Databases – Service Group

The Service Group lets you specify a Port and assign it to a group name for easy use when configuring inbound and outbound policies for the firewall.

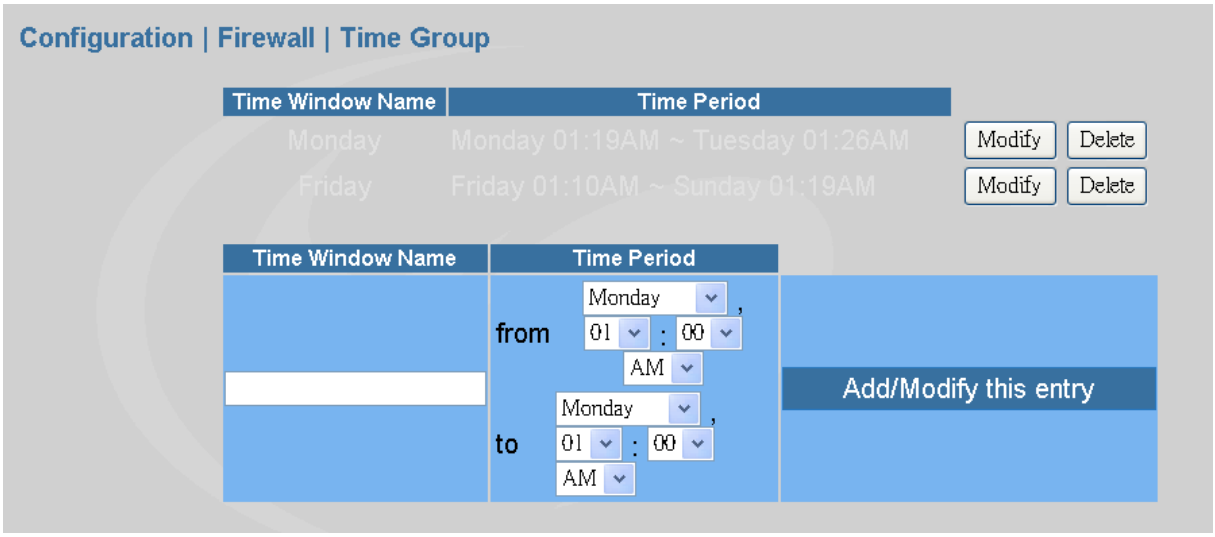


- Service Entry Name: This is the name you assign to the group containing the port number.

  The Service Name Entry can be up to 19 characters.
- TCP/UDP: This specifies whether the port goes through TCP or UDP.
- Port #: This is the port number associated with the group name. Range for Port # is 1 – 65535.

4.3.3.16.2.3 Firewall Databases – Time Window

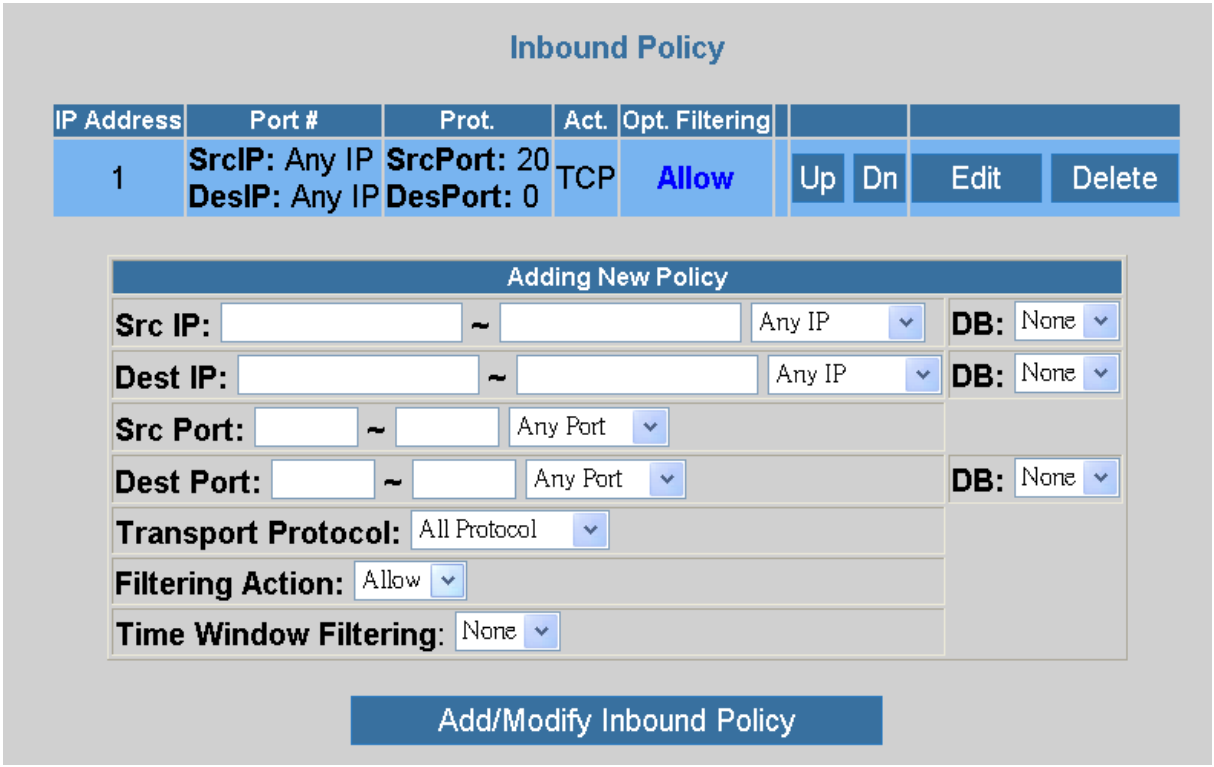
The Time Window lets you specify certain time periods and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.



- Time Window Name: This is the name you assign to the group that is given the time designation. The Time Window Name can be up to 19 characters.
- Time Period: This field allows you to specify the time period for both start time and end time by selecting the day, hour, minute, and AM/PM.

4.3.3.16.3.1 Inbound/Outbound Policies – Inbound Policy

The Inbound Policy allows you to filter inbound (from the WAN into the user side LAN) packets based on a set of rules. This enables you to deny access from different sources and thus increase security.

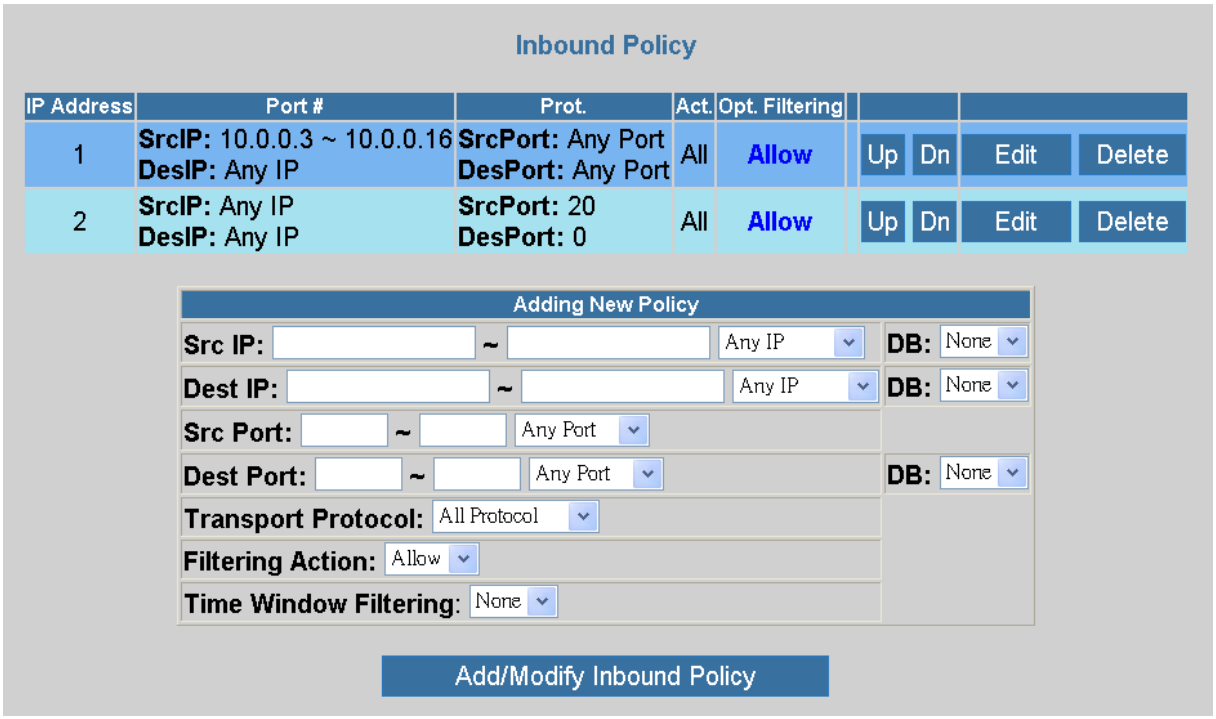


A table of inbound policies is displayed with the following information. If there are no policies, then a message stating "*No Entries in Inbound Policy Database*" will be displayed in place of the table.

- IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.
- Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.
- Prot.: Short for protocol, this is the protocol to which the policy applies.
- Act.: Short for action, this field specifies two possible actions: allow or deny.
- Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.
- Up: Clicking this button will move the corresponding policy up one space in the table.
- Dn: Short for down, clicking this button will move the corresponding policy down one space in the table.

Note: The Inbound Policy works in a Top-Down fashion according to the Inbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom. It is critical for both security and user accessibility to the WAN to have inbound policies in the correct order. See Section next section for an example of this.

- Edit: Clicking this button will display a table similar to the add table (see below) to the bottom of the policy table that will allow you to modify the corresponding policy.
- Delete: This will delete the corresponding policy.
- Add Inbound Policy: Clicking this button will bring up a table with all the add configurations as shown below:



- Src IP: This specifies the Source IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and Subnet Masks that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu. The dropdown menu has four options:
  - **Any IP**: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.
  - **Single IP**: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

- **IP Range**: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

- **Mask Range:** Selecting this will enable you to select a range of Subnet Masks to which the policy will apply. The first Subnet Mask in the range must be entered into the first IP Address entry field and the last Subnet Mask in the range must be entered into the second IP Address entry field.

◆ Dest IP: This specifies the Destination IP for the Inbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. See Src IP above for configuration detail.

◆ Src Port: This specifies the Source Port for the Inbound Policy. This is the external (WAN side, outside of the firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

- **Any Port:** Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

- **Single Port:** Selecting this will cause only one Port to be affected by the policy. This Port will need to be specified by the user in the first Port entry field.

- **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

- **Safe Ports:** Any port greater than 1024 (1025 – 65535) is considered a safe port.

◆ Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (LAN side, behind the firewall) Port that will be affected by the policy. See Src Port above for configuration detail.

◆ Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

◆ Filtering Action: This specifies what action the policy takes:

- **Allow:** Selecting this will cause the policy to allow packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

- **Deny:** Selecting this will cause the policy to deny packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

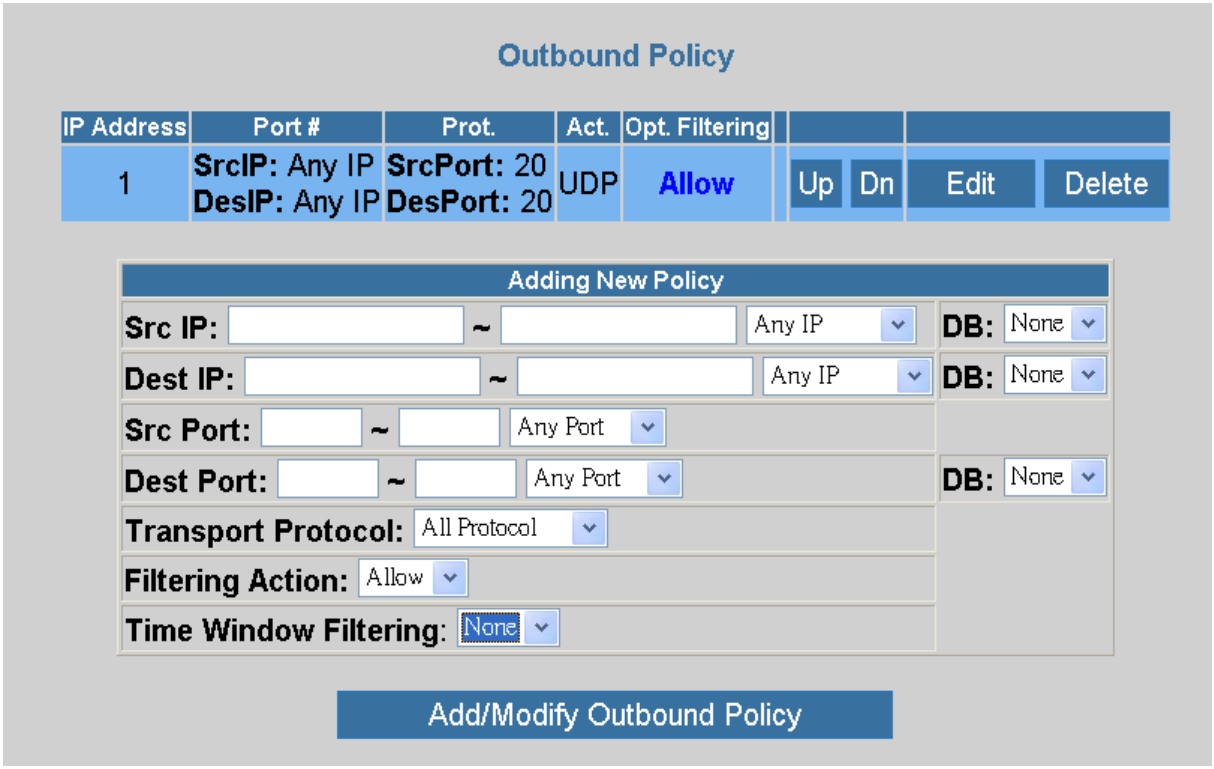
- Time Window Filtering: This field allows you to select a certain time frame from the Time Group in which this policy will be active. See section 4.3.3.16.2.3 for more information on Time Groups.

- DB: Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and a user-defined Service Group for the Dest Port. User defined IP and Service Groups are created in IP Group and Service Group pages, in this user guide.

  Note: Source and Destination IP Addresses, Subnet Masks, and Ports are reversed between Inbound Policy and Outbound Policy. For Inbound Policy, the source is on the WAN side and the destination is on the LAN side. For Outbound policy, the source is on the LAN side and the destination is on the LAN side.

4.3.3.16.3.2 Inbound/Outbound Policies – Outbound Policy

The Outbound Policy allows you to filter outbound (from the user side LAN to the WAN) packets based on a set of rules. This enables you to deny access to different sources and thus increase security.

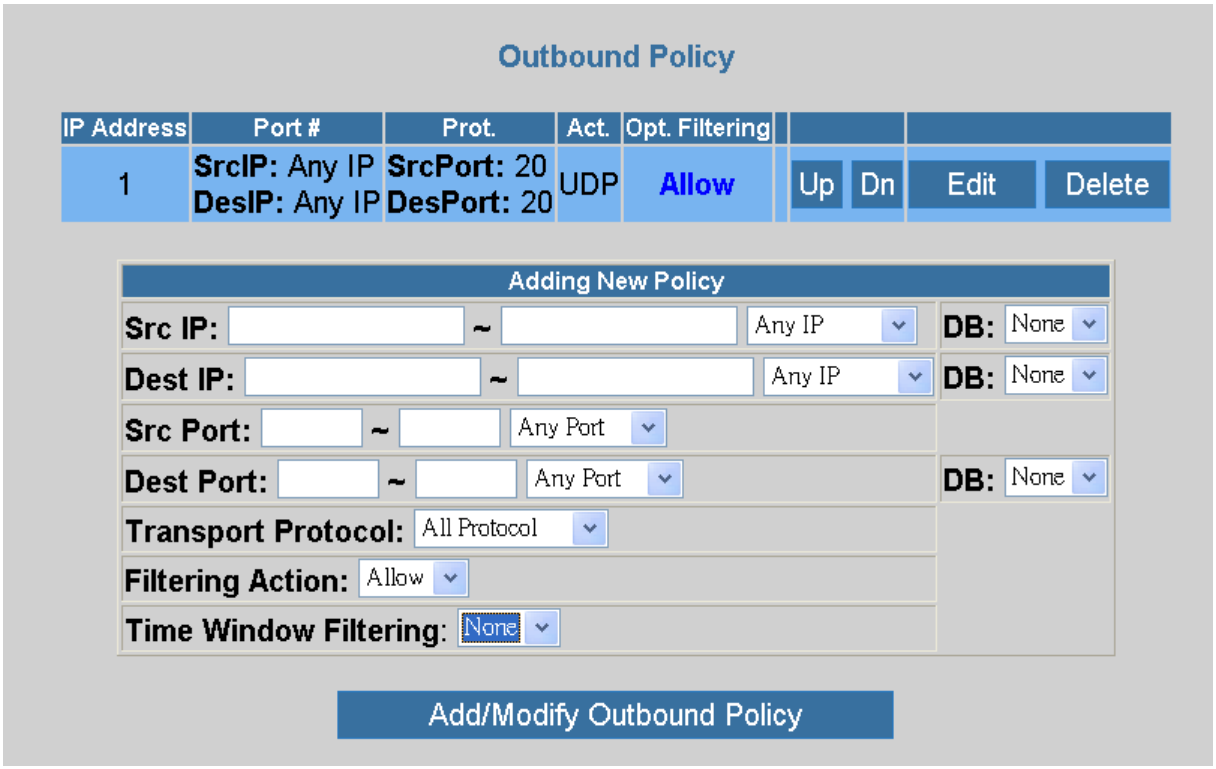


A table of outbound policies is displayed with the following information. If there are no policies, then a message stating “No Entries in Outbound Policy Database” will be displayed in place of the table.

- IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.
- Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.
- Prot.: Short for protocol, this is the protocol to which the policy applies.
- Act. Short for action, this field specifies two possible actions: allow and deny.
- Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.
- Up: Clicking on this button will move the corresponding policy up one space in the table.
- Dn: Short for down, clicking on this button will move the corresponding policy down one space in the table.

Note: The Outbound Policy works in a Top-Down fashion according to the Outbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom. It is critical for both security and user accessibility to the WAN to have outbound policies in the correct order. See Section below for an example of this.

- Edit: Clicking this button will display a table similar to the add table (see next page) to the bottom of the policy table that will allow you to modify the corresponding policy.
- Delete: This will delete the corresponding policy.
- Add Inbound Policy: Clicking on this button will bring up a table with all the add configurations as shown below:



- Src IP: This specifies the Source IP for the Outbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu. The dropdown menu has four options:
  - **Any IP**: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.
  - **Single IP**: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

- **IP Range**: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

- **Mask Range:** Selecting this will enable you to select a range of Subnet Masks to which the policy will apply. The first Subnet Mask in the range must be entered into the first IP Address entry field and the last Subnet Mask in the range must be entered into the second IP Address entry field.

◆ Dest IP: This specifies the Destination IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and subnet mask(s) that will be affected by the policy. See Src IP above for configuration detail.

◆ Src Port: This specifies the Source Port for the Inbound Policy. This is the internal (LAN side, behind firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

- **Any Port:** Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

- **Single Port:** Selecting this will cause only one Port to be affected by the policy. This Port will need to be specified by the user in the first Port entry field.

- **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

- **Safe Ports:** Any port greater than 1024 (1025 – 65535) is considered a safe port.

◆ Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (WAN side, outside of the firewall) Port that will be affected by the policy. See Src Port above for configuration detail.

◆ Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

◆ Filtering Action: This specifies what action the policy takes:

- **Allow:** Selecting this will cause the policy to allow packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

- **Deny:** Selecting this will cause the policy to deny packet transfer from the **Src**

◆ IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.

- Time Window Filtering: This field allows you to select a certain time frame from the Time Group in which this policy will be active. See section 6.6 for more information on Time Groups.

- DB: Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and a user-defined Service Group for the Dest Port. User defined IP and Service Groups are created in IP Group and Service Group pages.

Example : Inbound/Outbound Policies Sample Configuration

This is a sample Inbound/Outbound configuration meant to guide you in making your own configurations. This configuration does not necessarily provide proper security, it is meant only as a sample to display the functionality of the Inbound and Outbound Policies.

A. Inbound Policy :

Sample Configuration : You want your firewall to have the following properties:

- Accept all http IP addresses, except for 204.35.82.1

- Grant FTP access from 101.64.35.4 (external) to 10.0.0.3, 10.0.0.4, 10.0.0.5, and 10.0.0.6 (all internal).

- Deny all access to FTP Server 10.0.0.6 on the weekend.

Converting the access requirements from above so that the Inbound Policy can understand them yields the following:

- Deny access from any Src (WAN) IP to any Des (LAN) IP through any source or destination port and through all protocols.

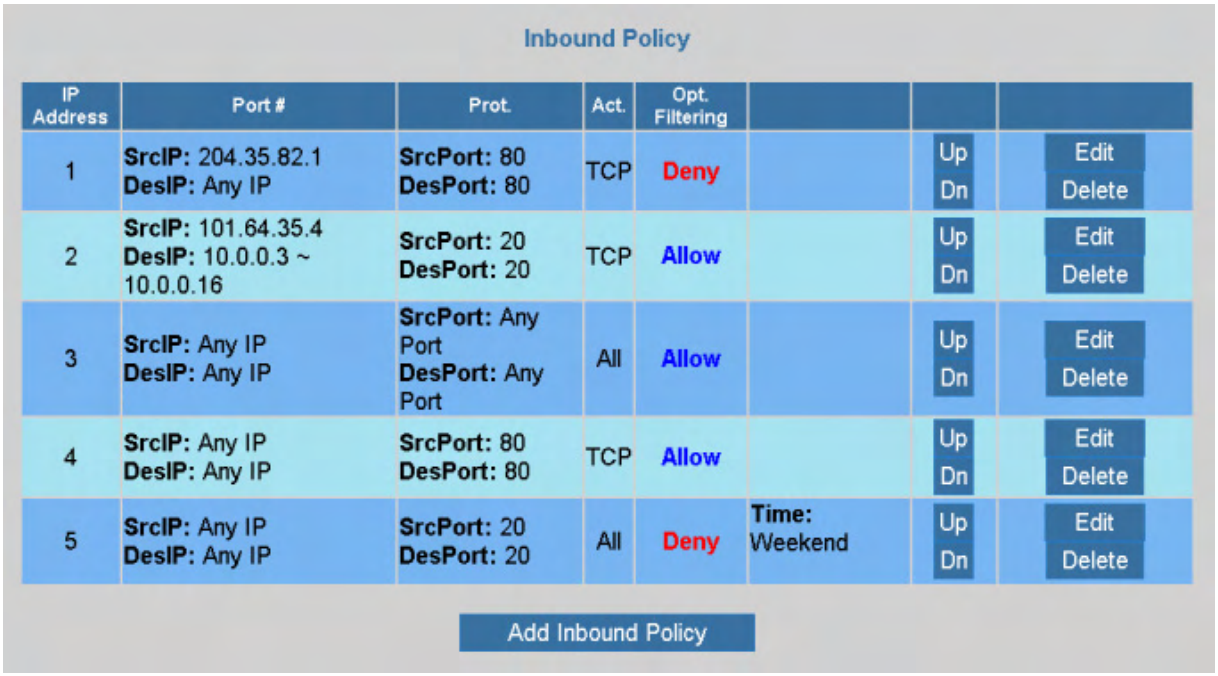
- Allow access from any Src (WAN) IP to any Des (LAN) IP through port 80 (HTTP), through TCP.

- Deny access from Src (WAN) IP 204.35.82.1 to any Des (LAN) IP through port 80 (HTTP), through TCP.

- Allow access from Src (WAN) IP 101.64.35.4 to Des (LAN) IP 10.0.0.3 ~ 10.0.0.6 through port 20 (FTP), through TCP.

- Deny access from any Src (WAN) IP to DB FTP (defined as) IP through any source or destination protocol and through all protocols during time period WEEKEND, where WEEKEND is defined in the Time Group as Saturday, 12:00AM to Sunday, 11:59PM. It does not matter which order you input these in as long as you sort them into the correct order once you are finished.

The configuration should look like the following when complete:



Inbound Policy

IP Address	Port #	Prot.	Act.	Opt. Filtering			
1	**SrcIP:** 204.35.82.1 **DesIP:** Any IP	**SrcPort:** 80 **DesPort:** 80	TCP	Deny		Up Dn	Edit Delete
2	**SrcIP:** 101.64.35.4 **DesIP:** 10.0.0.3 ~ 10.0.0.16	**SrcPort:** 20 **DesPort:** 20	TCP	Allow		Up Dn	Edit Delete
3	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** Any Port **DesPort:** Any Port	All	Allow		Up Dn	Edit Delete
4	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** 80 **DesPort:** 80	TCP	Allow		Up Dn	Edit Delete
5	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** 20 **DesPort:** 20	All	Deny	**Time:** Weekend	Up Dn	Edit Delete

Add Inbound Policy

Note: It should be clear now how critical it is to sort the policies in the correct order. For example, if policies one and two were switched, there would be NO HTTP access to any computer in the LAN. This would make web browsing impossible.

B. Outbound Policy :

Sample Configuration: You want to deny all access to the WAN except for the following:

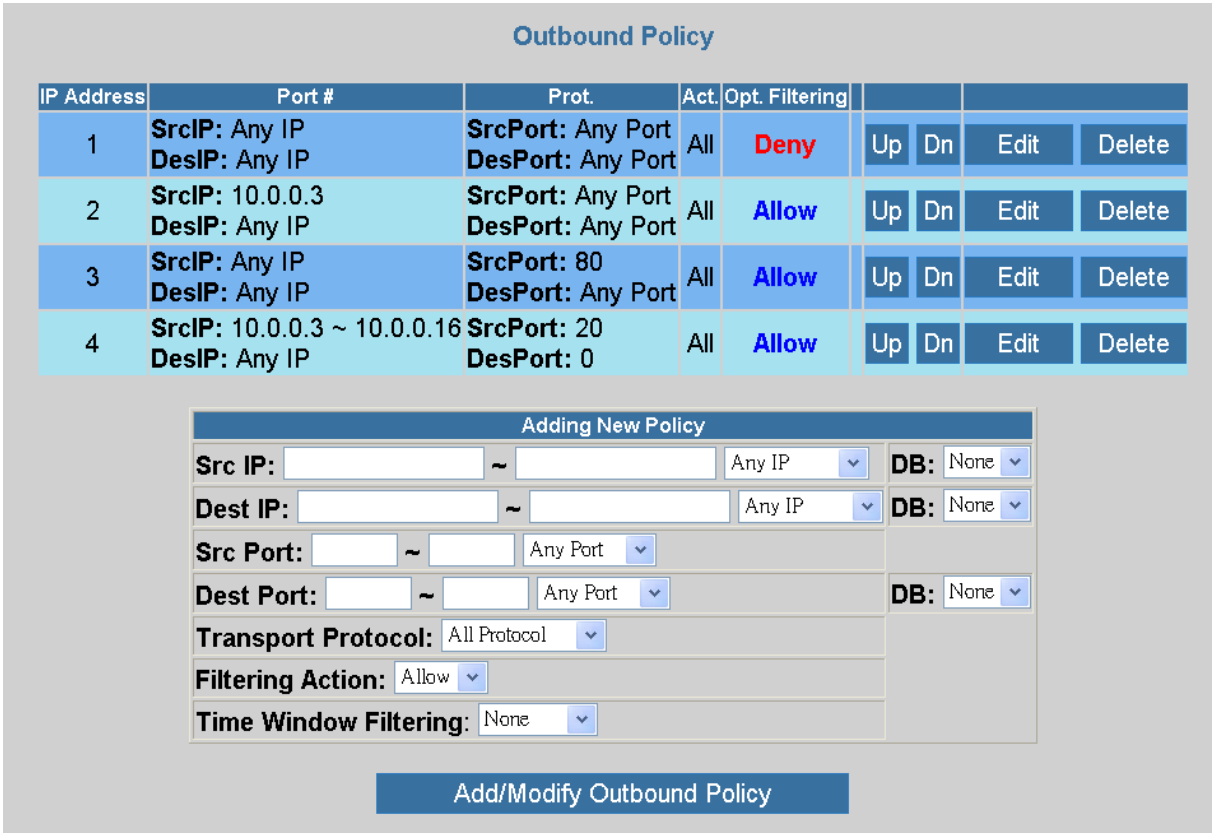
- HTTP access from any IP through TCP.
- Any access from 10.0.0.3 through any protocol.
- FTP Access from 10.0.0.3~10.0.0.6 through any protocol.

Converting the access requirements from above so that the Outbound Policy can understand them yields the following:

- Deny all access from any Src (LAN) IP to any Des (WAN) IP through any source or destination port and through any protocol.
- Allow access from Src (LAN) IP 10.0.0.3 to any Des (WAN) IP through any port through any protocol.
- Allow access from any Src (LAN) IP to any Des (WAN) IP through port 80 (HTTP), through TCP.

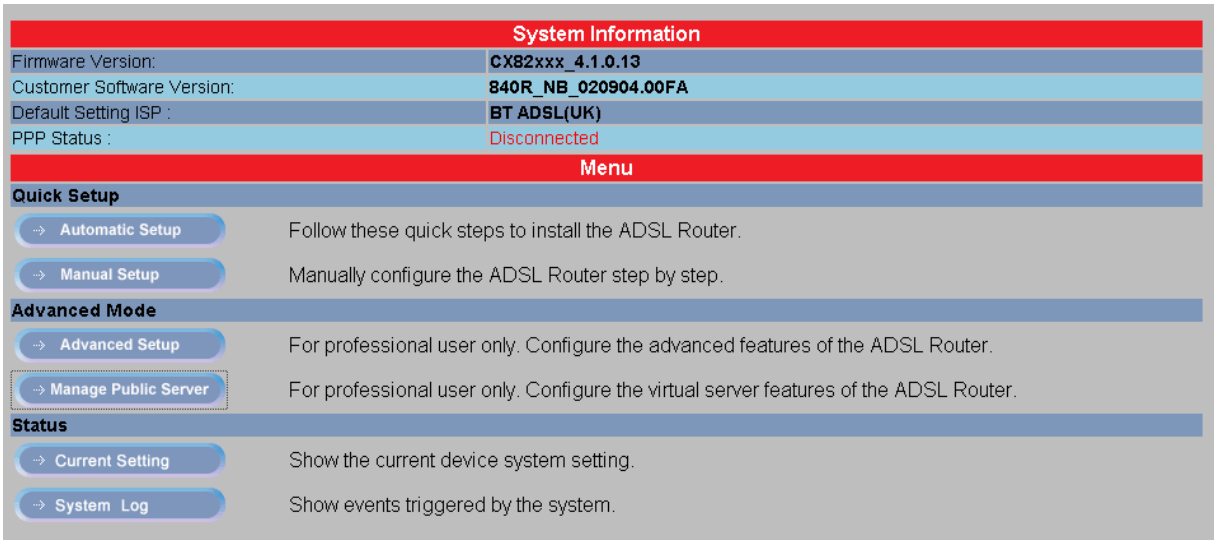
- Allow access from Src (LAN) IP range 10.0.0.3~10.0.0.6 to any Des (WAN) IP through port 20 (FTP), through any protocol.

The configuration should look like the following when complete:



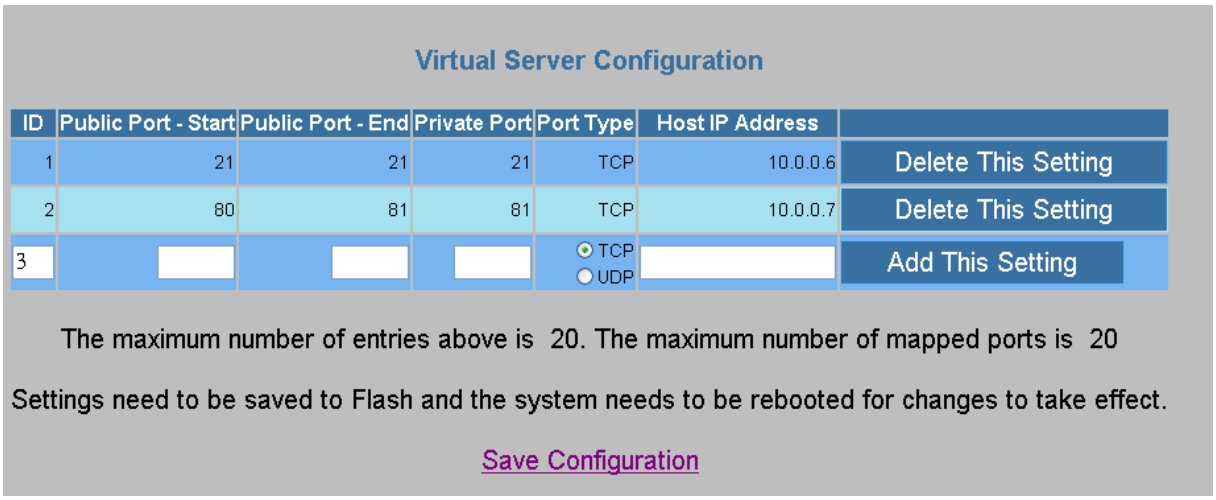
4.3.4 Advanced Mode – Manage Public Servers

The Manage Public Severs are used for port forwarding from the WAN to LAN networks.



The **Virtual Server Configuration** page allows you to set the configuration of the Virtual Server. All UDP/TCP ports are protected from intrusion. If any specific local PCs need to be mapped to the UDP/TCP port on WAN side, please input the mappings here.

Note : There can be up to 20 different Virtual Server Configurations.



- ID: This is the ID number corresponding to the Virtual Server configuration.
- Public Port - Start: This field allows you to enter the port number of the Public Network (WAN or external network). If you are entering a range of ports, this is the first port.
- Public Port - End: This field represents the last port number in a port range. If you only want one port number (no port range), simply enter the same number here as in the Public Port – Start field.

Note : The maximum number of the mapped Port is 20.

- Private Port: This field allows you to enter the port number of the Private Network (LAN or internal network). In most cases, the private port number is same as public port number. This port number cannot be seen from the WAN side.

- Host IP Address: This field allows you to enter the private network IP address for the particular server.
  Well-known TCP/IP ports are listed in Table below :

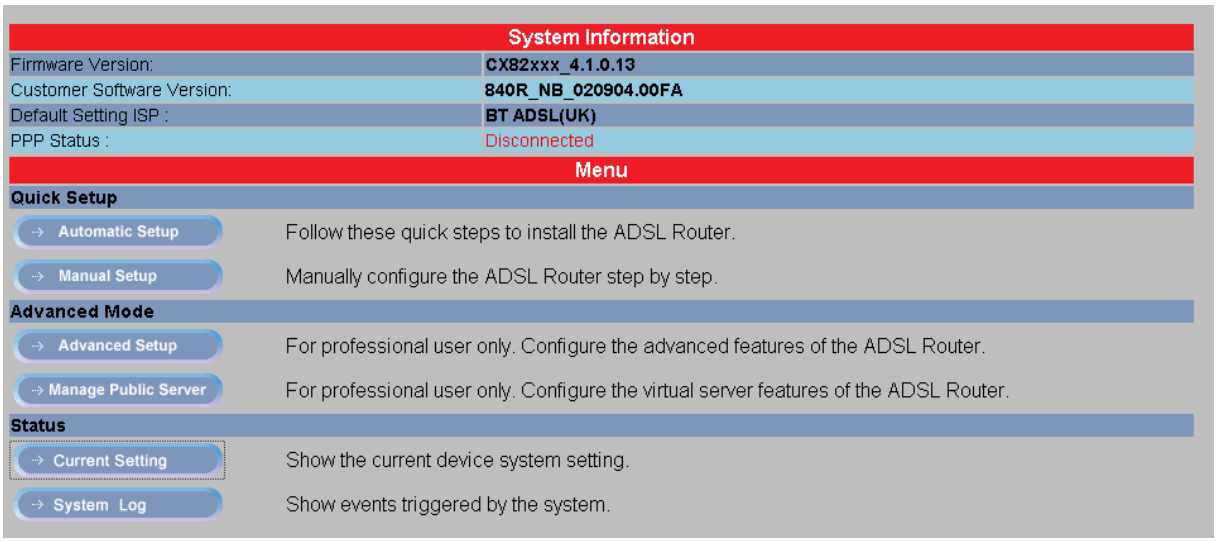
Port	Protocol	TCP	UDP
20	File Transfer Protocol (FTP) Data	X	
21	FTP Commands	X	
23	Telnet	X	
25	SMTP	X	
43	Whois	X	
53	Domain Name System (DNS)	X	X
69	Trivial File Transfer Protocol (TFTP)		X
70	Gopher	X	
79	Finger	X	
80	HTTP	X	
110	POP3	X	
111	SUN Remote Procedure Call (RPC)		X
115	SFTP	X	
119	Network News Transfer Protocol (NNTP)	X	
123	Network Time Protocol (NTP)	X	X
144	News	X	
161	Simple Network Management Protocol (SNMP)		X
162	SNMP traps		X
179	Border Gateway Protocol (BGP)	X	
443	Secure HTTP (HTTPS)	X	
513	rlogin	X	
514	rexec	X	
517	talk	X	X
518	ntalk	X	X
520	Routing Information Protocol (RIP)		X
1701	Layer 2 Tunneling Protocol (L2TP)		X
2000	Open Windows	X	X
2049	Network File System (NFS)	X	
6000	X11	X	X

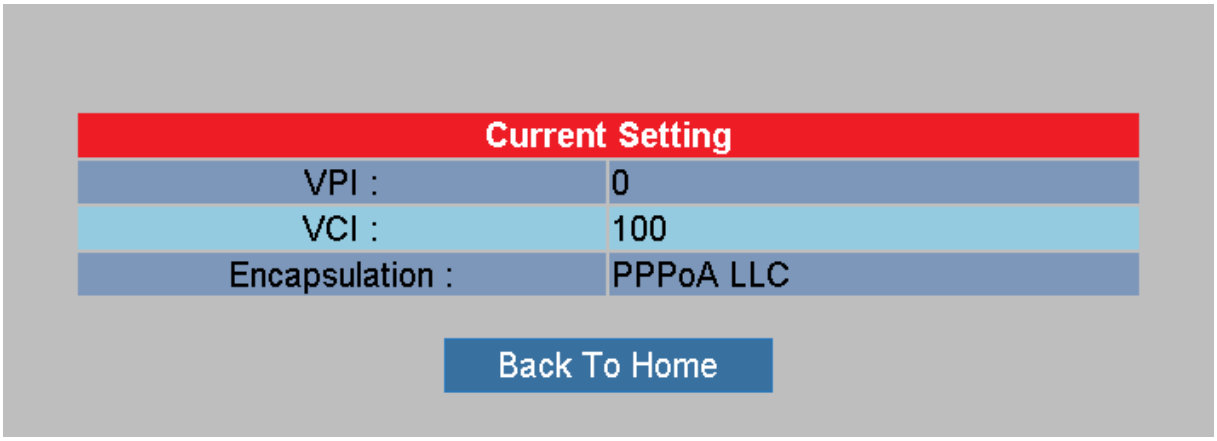
4.4 Status

Shows all the Configuration/Setting/Status of the ADSL Router.

4.4.1 Status – Current Setting

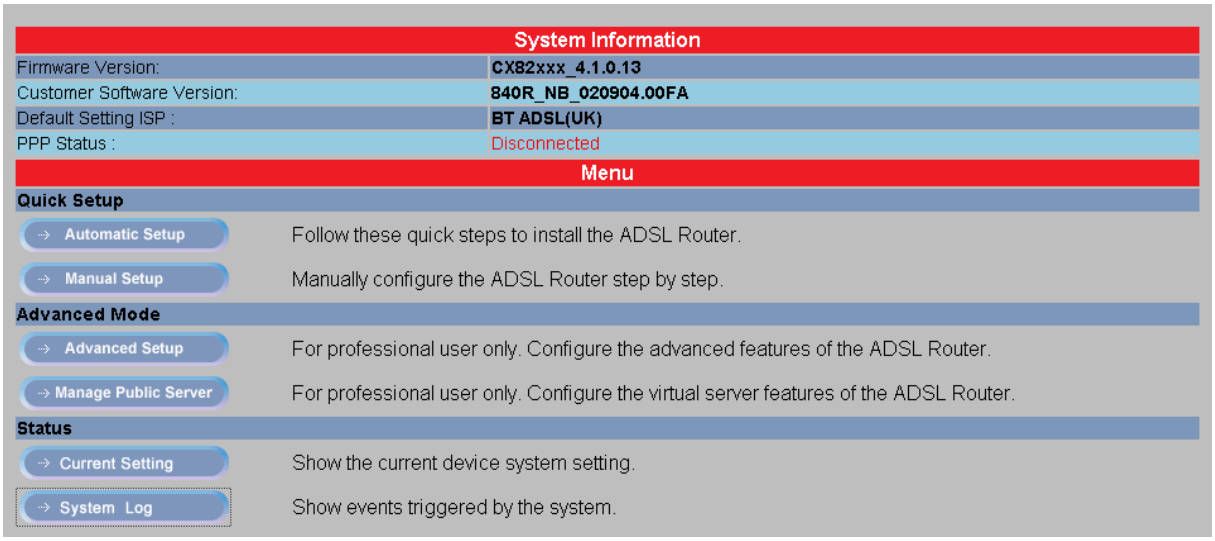
Click **"Current Setting"** to display the current Configuration/Setting of the ADSL Router.

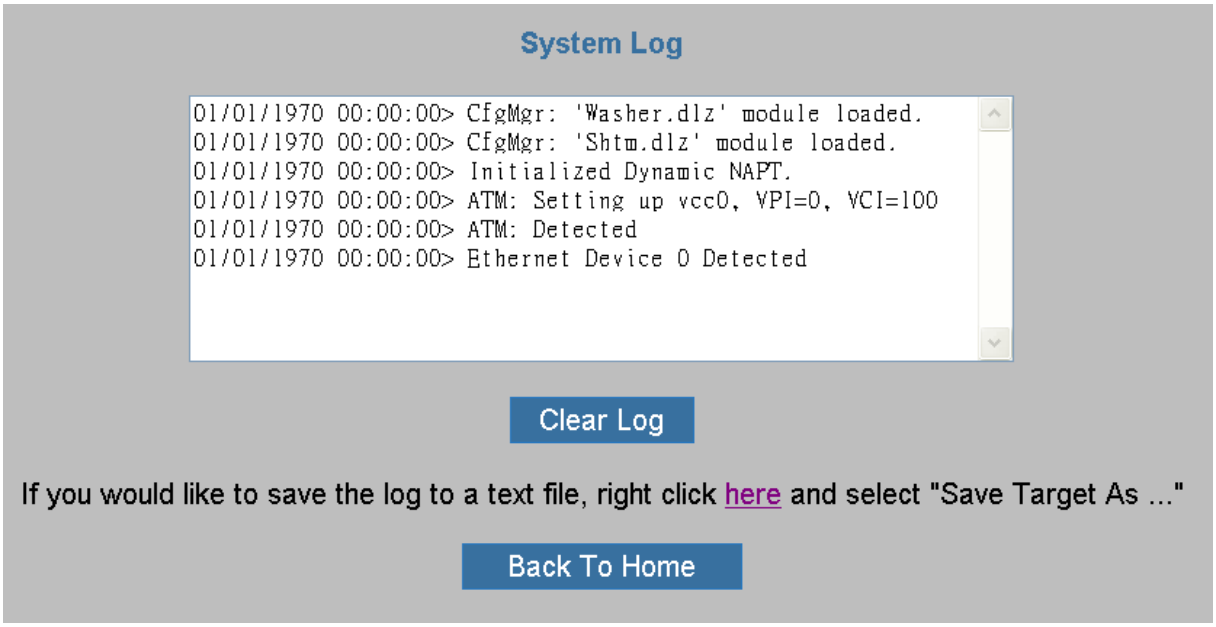




4.4.2 Status – System Log

The **System Log** page shows the events triggered by the system. This page contains information that is dynamic and will refresh every 5 seconds.




System Log
01/01/1970 00:00:00> CfgMgr: 'Washer.dlz' module loaded.
01/01/1970 00:00:00> CfgMgr: 'Shtm.dlz' module loaded.
01/01/1970 00:00:00> Initialized Dynamic NAPT.
01/01/1970 00:00:00> ATM: Setting up vcc0, VPI=0, VCI=100
01/01/1970 00:00:00> ATM: Detected
01/01/1970 00:00:00> Ethernet Device 0 Detected
Clear Log
If you would like to save the log to a text file, right click here and select "Save Target As ..."
Back To Home

- Clear Log: This field allows you to clear the current contents of the System Log.
- Save Log: This field allows you to save the current contents of the System Log by right click **"HERE"** and select **"Save Target As"** to save it into a text file.

- The System Log records:
  - ADSL Layer :
    - ADSL Link detected
    - ADSL Link connected
    - ADSL Link disconnected
  - ATM Layer :
    - ATM detected
    - ATM connected
    - ATM disconnected
    - ATM setting up VPI/VCI
  - PPP Layer :
    - PPP authenticated
    - PPP invalid user name or password
    - PPP unable to connect with PPP server
  - IP Layer :
    - IP protocol up
    - PPP IP address
    - PPP Gateway IP address PPP DNS Primary IP address
    - PPP DSN Secondary IP address

Appendix A : Network Address Translation

Network Address Translation (NAT) translates the IP address a network (LAN) to a different IP address known by another network (WAN). This gives an outside network the ability to distinguish and communicate with a device on the inside network, as the inside network has a private set of IP addresses assigned by the DHCP server, which are not know to the outside network.

The rise of NAT and increasing use of NAT come from several factors.

- World shortage of IP Addresses: Public IP addresses need to be used in the public domain. However, the limited supply of public IP addresses cannot satisfy the increasing demand. NAT allows multiple IP nodes in the private domain to share one public IP address. This conserves the pool of public IP address, and makes private IP addresses reusable in other private domains.

- Privacy / Security: Concern in privacy and security arises when exposing IP addresses in a private network to the public domain. NAT automatically provides firewall-style protection by only allowing connections originated from the private network and not allowing attackers on the public domain to distinguish individual IP addresses of computers internal to the network.

- Administrating external network topology changes: Without NAT, when the network topology of the public domain changes, the address assignment for the local domain would be forced to change accordingly. NAT separates the private network from the public domain. Thus, changes of public domain network topology can be hidden from users within the private domain.

NAT operation is based on where the traffic is initiated instead of the physical packet direction.

Outbound sessions are initiated from the private network accessing the external network. For example, an FTP session initiated from a host in the private network to access the FTP server through the internet is considered an outbound session. This session includes bi-directional packet exchange. The primary NAT function allows outbound sessions so that hosts in a private network can transparently access the external network.

Inbound sessions are initiated from the external network accessing the private network. For example, an FTP session initiated by a host from the external network to access the FTP server residing in the private network is considered an inbound session. NAT usually blocks all inbound sessions. Various implementations may be added to extend the NAT function and enable selective inbound sessions to allow access to local hosts from outside networks.

A.1 Basic NAT

Basic Network Address Translation (NAT) enables outbound sessions for the hosts in a private network to gain 0access the external network.

Facts of Basic NAT:

- Basic NAT allows hosts in a private network to transparently access the external network.
- Basic NAT maps only one IP addresses in the private domain to each IP address in the public domain. This is known as peer-to-peer mapping (1x1). For each WAN interface, only one local PC IP address can be associated with each WAN interface.
- Translation in Basic NAT is limited to IP addresses alone.
- The number of nodes allowed to simultaneously access the external network is limited by the number of IP addresses assigned in the public domain.

A.2 Static NAPT

NAPT, also known as NAT-PAT, stands for Network Address Translation and Port Address Translation. An extension of Basic NAT, NAPT enables outbound sessions so that the hosts in a private network to access the external network.

Facts of NAPT:

- NAPT multiplexes traffic from the internal network and presents it to the Internet as if it is coming from only one IP address.
- Translation in NAPT is extended to include IP address and Transport identifier such as TCP/UDP port or ICMP query ID.
- NAPT maps multiple IP addresses and their TCP/UDP ports in the private domain to a single IP address and its TCP/UDP ports in the public domain. This is known as a multiple-mapping mechanism. For each WAN Interface, more than one local PC can be associated with one WAN Interface.
- NAPT allows multiple nodes in a local network to simultaneously access remote networks using the single IP address assigned to their router.

A.3 Functional Descriptions

This section describes various NAT mechanisms for both outbound and inbound session operations. Together, they provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.

The NAT module allows outbound access with either static or dynamic sessions. Inbound access is normally blocked but selective inbound sessions may be enabled.

A.3.1 Outbound Access

The NAT module implements two modes for outbound sessions: NAT mode and NAPT mode.

- NAT Mode: NAT mode implements the Basic NAT functionality.

  1. Static session mapping is required for any local host to access the public domain.
  2. Only one local host can be mapped to each WAN Network Interface.
  3. If multiple local hosts are mapped to the same WAN Network Interface, only the first one will take effect. All other entries are marked with * indicating that the entries will not take effect.

- NAPT Mode: The NAPT mode implements the NAPT functionality.

  1. Multiple local hosts can access the public domain using the same WAN Network Interface.
  2. Two types of sessions may be created in this mode: dynamic and static. Static sessions take priority over dynamic sessions.
  3. Static session mapping is NOT required for any local host to access the public domain. Static session mapping can be configured to fix the WAN Network Interface that a local host must use to access the public domain. This does not limit the number of local hosts this WAN Network Interface can serve in the NAPT mode.
  4. Dynamic session mapping is created automatically. When a packet from the LAN is processed and if no existing NAT session can be found, then a dynamic session is created on a per packet basis based on the Route Table. That is, the destination IP address is used to find the appropriate Network Interface to deliver the packet to, based on the Route Table. If the Network Interface is a WAN interface, then the IP address of the WAN interface is used to create the session dynamically and the Address/Port translation is performed. Thus, packets originating from one local host may be mapped to multiple WAN interfaces.
  5. If the packet cannot be routed based on the Route Table when trying to create a dynamic session, then no dynamic session is created and the packet is not processed by NAT. This is different than the obsolete one-WAN static NAPT mode where a hidden “default session” maps all LAN clients to only one WAN. The “default route” of the Route Table serves a similar purpose through dynamic sessions.
  6. A dynamic session is deleted dynamically either when the connection is completed or when the inactivity timer expires. Thus, changes to the Route Table may not change the NAT packet forwarding on existing sessions. This may create confusion in some cases. For example, there are two WAN connections: WAN1 is the default route and goes to internet, WAN2 has an internal server behind it and a manual route entry is entered to reach that internal server. If WAN2 has a dynamic connection such as PPP or DHCP and a LAN client tries to ping that internal server before WAN2 is connected, then the ping request is routed to WAN1 based on the route table. While the continuous ping requests keeps going, WAN2 is connected. However, the ping requests are continually forwarded to WAN1 and they cannot reach the internal server. The reason is that when the first ping request was generated, NAT creates a dynamic session, based on the route table, to forward it to WAN1. Since the ping failed, the ping session was never completed, so the dynamic session stays in NAT until it expires. Therefore, each ping request refreshes the timer of that dynamic session in NAT so the session never expires. In this case, stop the

ping for a period of time, let the session expire, then restart the ping. The expiration time differs from protocol to protocol.

7. With dynamic WAN interfaces, the Route table changes as links go up and down. Since NAPT is based on Route Table, NAT packet forwarding may behave differently from time to time.

- Static Session Mapping: Static session mapping is used in both NAT mode and NAPT mode.

1. The static session mapping used in NAT mode and NAPT mode are the same except for one difference. Only one session mapping is effective per WAN Network Interface in the NAT mode, while there is no limit in the NAPT mode.
2. Session mapping maps a local host IP address to a WAN Network Interface. You must first create a Session Name and associate it with the intended WAN Network Interface. Then you can map local host IP addresses to that Session Name.
3. Depending on the memory resource availability:

    i. Up to 64 Session Names can be created for each WAN Network Interface.
    ii. Up to 64 Session Names can be created in the system.
    iii. Up to 253 Local host IP mappings can be created for each Session Name.
    iv. Up to 253 Local host IP mappings can be crated in the system.

A.3.2 Inbound Access

Inbound access is normally blocked; however, selective inbound sessions may be enabled. The NAT module implements two types of inbound access control: Virtual Server and Demilitarized Zone (DMZ).

- Virtual Server: The term “Virtual Server” came from the concept of subdividing one physical system into multiple “virtual” systems.

    1. The NAT module provides Virtual Server service through static inbound NAT sessions.
    2. Each Virtual Server statically maps a local host per service TCP/UDP port of the WAN interface.
    3. Multiple mappings may be mapped to the same local host.
    4. A static inbound NAT session includes the protocol type (TCP or UDP) of the incoming packet, the public port number the packet is destined to, and the IP address and the port number of the virtual server (i.e. the local host).
    5. Contiguous public ports form a group that can be mapped to a virtual server from the WEB by entering the port range for that group (see the **Virtual Server** configuration page).
    6. Depending on the memory resource availability, up to 20 public ports group can be created. However the maximum number of mapped ports is 20.

- Demilitarized Zone (DMZ): The NAT module provides the functionality of a “NAT box” DMZ, not a “real” DMZ. The general definition of a “real” DMZ is a section of a network between exterior and interior firewalls where publicly accessible servers are usually placed. A “real” DMZ provides separation of the servers placed within it and the private network, a “NAT box” DMZ does not.

    1. The DMZ implemented in the NAT module allows one local host to be exposed to the Internet. i.e. Only one DMZ host can be configured in the system.
    2. When an incoming packet from the public domain cannot be resolved by NAT Sessions and Virtual Servers, it is forwarded to this “default host.”
    3. Note that it allows full bi-directional public access, and address translation still takes place.
    4. One popular use of this feature is when inbound connections to a range of ports are required and it is impractical or impossible to accommodate them via port mappings.
    5. The DMZ opens all ports on this particular local host to all unsolicited traffic, therefore posing some security risk. This means that the protection of NAT is removed from that local host and external hosts can initiate conversations with it on any port.

Appendix B Frequently Asked Questions

The Frequently Asked Questions addresses common questions regarding ADSL Router settings. Some of these questions are also found throughout the guide, in the sections to which they reference.

Q1. How do I determine if a link between the Ethernet card (NIC) and the ADSL Router has been established?

ANS: A ping test would determine if a connection is established between your ADSL Router and computer. Using, the ping command, ping the IP address of the ADSL Router, in this case, 10.0.0.2 (default). For more information on Ping Testing, refer to Appendix C: Troubleshooting Guide. Alternatively, if the Ethernet LINK LED is solidly on, then the Ethernet link is established.

Q2. How do I determine if a link between the ADSL Router and the Internet has been established?

ANS: Similar to the previous question, a ping test would determine whether or not a connection is established. However, this time use a URL instead of and IP Address, such as www.google.com. Alternatively, if the DSL LED is solidly on, then the ADSL link is established.

Q3. What can I do to ensure an always-on connection with my PPP session?

ANS: There are two things you should do: 1) Make sure you have ‘0 ‘in the Disconnect Timeout field. This will make sure that the PPP session is not disconnected from the User side. 2) Make sure the Automatic Reconnect box is checked. This will cause the ADSL Router to automatically reconnect if the connection is severed from either the ISP side or the user side.

Q4. How do I create a PPP session and connect it to the ISP?

ANS: To create and connect a PPP session, follow the steps below:

- First you must create a PPP account. To do this, go to PPP Configuration page and click on PPP Account Configuration. Enter the appropriate Acct ID, User Name, and Password, make sure Add/Modify is currently selected in the dropdown menu, and click Submit.
- Got back to the PPP Configuration Page by clicking Go back to PPP Configuration. Type in an appropriate Session Name and select the account you just created in the Account to Use dropdown menu. Everything else has default values, which you can modify to suit your needs. Make sure Add/Modify is currently selected in the dropdown menu, and click Submit.
- The PPP session has been created. Now you must go to the PPP Status page, select the connection (session), and click Execute. The PPP session should then connect.

Q5. Where can I download the free software to test IGMP?

ANS: Please go to this link http://manimac.itd.nrl.navy.mil/**MGEN**/.

Q6. How do I forward packets with MAC address 000002fa6fab to destination MAC 000003dc8faa through IP protocol?

ANS: First go to the **Bridge Filtering page** under **Configuration**. Then type 000002fa6fab in **the ID Source MAC** field, 000003dc8faa in the **Destination MAC** field, and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field. Then select **Forward** and click **Submit**.

Q7. How do I block packets from MAC address 000002fa6fab through IP protocol?

ANS: First go to the **Bridge Filtering page** under **Configuration**. Then type 000002fa6fab in **the ID Source MAC** field and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field.

Then select **Block** and click **Submit**.

Q8. How do I block incoming packets with destination MAC address 000003dc8faa through IP protocol?

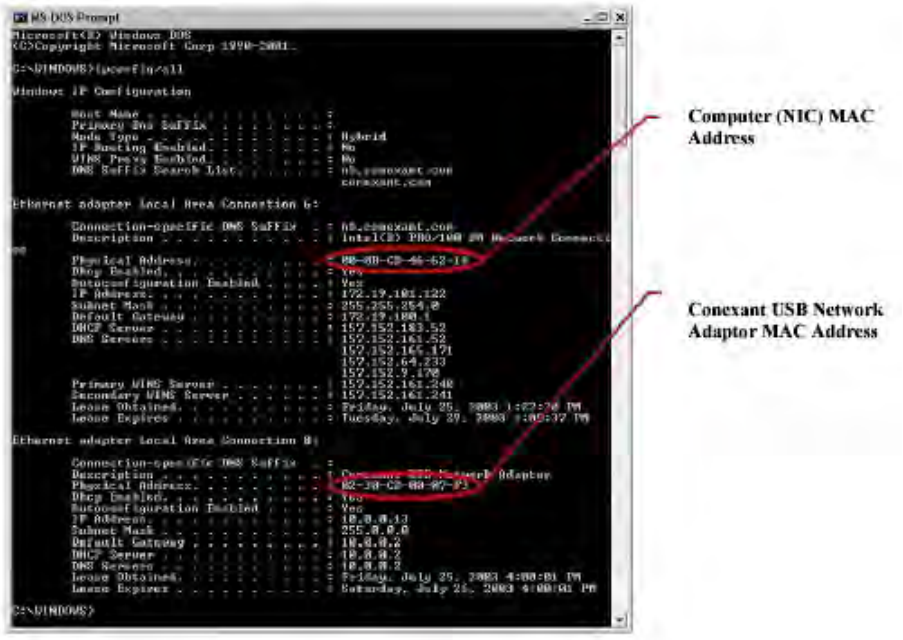
ANS: First go to the **Bridge Filtering page** under **Configuration**. Then type 000003dc8faa in the **Destination MAC** field, and 0800 in the **Type** field. If bridge filtering is not already enabled, select **Yes** under the **Enable Bridge Filtering** field.

Then select **Block** and click **Submit**.

Q9. How can I find/verify my ADSL Router and/or computer Ethernet MAC Address?

ANS: Follow the following instructions for the appropriate operating system:

- Windows NT/2000/XP : Click on Start Menu→(All) Programs→Accessories→Command Prompt (MS-DOS Prompt in NT). Once in the command prompt, type ipconfig/all and press enter. There should be at least 3 Tables of information. The first one should be labeled Windows IP Configuration. The other two are for your Network Interface Card (NIC) and your ADSL Router. You should be able to find out which one is which by looking at the Description field. The respective MAC addresses will be located in the Physical Address field.
- Windows 95/98/98SE/Me: Click on Start Menu→Run. Type winipcfg and click OK. Click more info. To check the MAC Address for the ADSL mode, select the ADSL Router on the dropdown menu. The MAC Address is labeled as the Adaptor Address. To find the computer (NIC) address, select the NIC device. The MAC Address is labeled as the Adaptor Address.
- Mac OS 7.6.1 and above (Not OS X): Click on the Apple menu→Apple System Profiler. Click the Network Overview arrow and then the AppleTalk arrow. The E-MAC Address is the 12-character Hardware Address.
- Mac OS X: Click on the Dock→System Preferences. Then click on Network. Under the Configure drop-down tab, choose Built-in Ethernet or Ethernet. Select the TCP/IP Tab. The E-MAC Address is the 12-digit Hardware Address. Click on Save and close the Network pane.



Appendix C Troubleshooting Guide

The Troubleshooting Guide provides answers to common problems regarding the ADSL Router settings, connections, and computer settings.

I changed the LAN IP Address in the LAN configuration page and my PC is no longer able to detect the ADSL Router.

After changing the LAN IP Address of the ADSL Router, you must do one of the following things before a PC is able to recognize the ADSL Router:

- Open the MS-DOS prompt and run ipconfig/release followed by ipconfig/renew.
- Reboot the computer.
- Disconnect the ADSL Router from the computer, and then reconnect it.
- Turn off the ADSL Router and then turn it back on.

Only one computer can connect to the ADSL Router or my ADSL Router can only recognize one computer.

There are several things to check:

- Make sure that the DHCP server is in Multiple User mode. To do this, go to the LAN Configuration page and under the User Mode field, select Multi-User.
- Make sure that the NAT is configured for multiple User IPs. To do this, go to the NAT configuration Page and change the NAT type of the particular session to Dynamic NAPT.
- If the problem persists, make sure that the computer that cannot connect has the appropriate network settings.

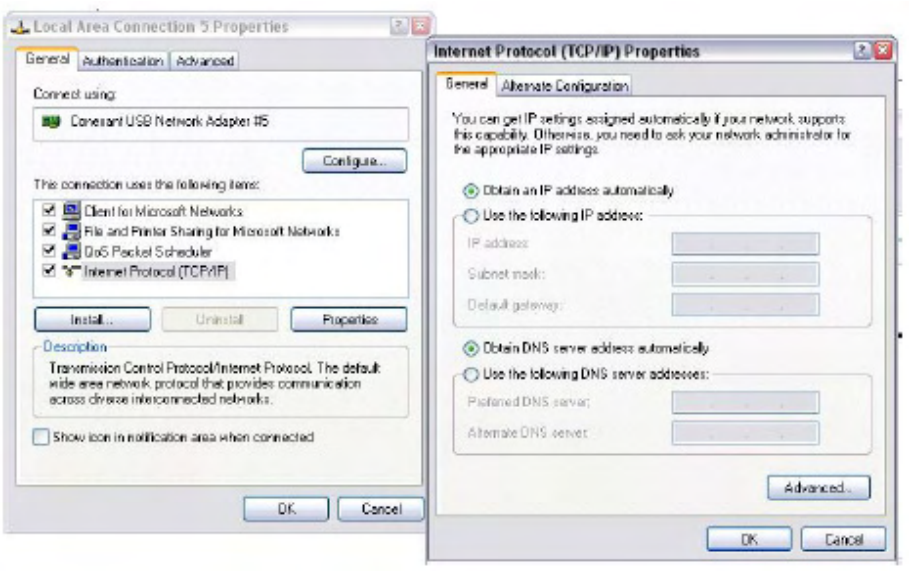
Appendix D Network Setup Guide

To configure your computer to connect to the Internet through a LAN, refer to the instructions or help guide provided with your Operating System.

It is recommended that the network address of the client PC to be configured as a dynamic IP address. This will give your DHCP server full control of IP Addresses and DNS Servers:

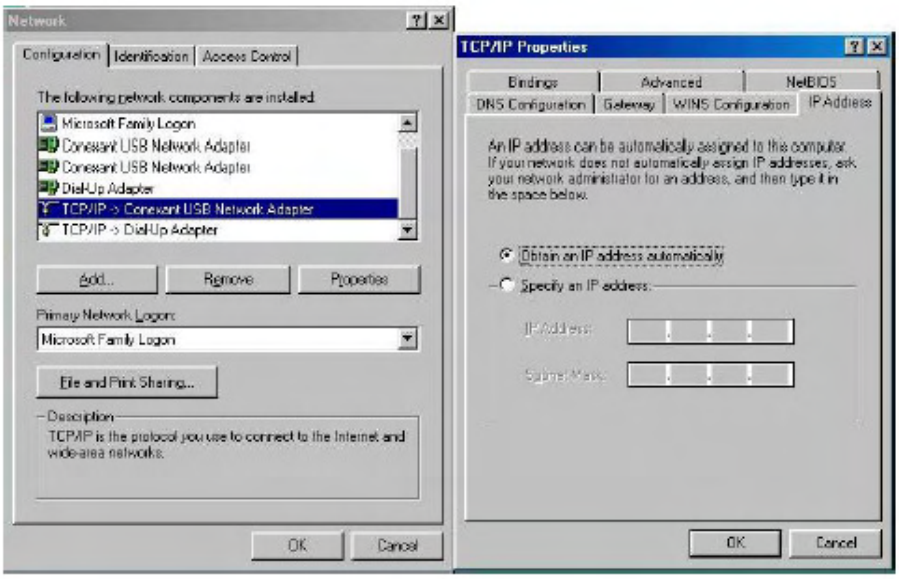
D.1 Windows XP/2000

- Click on Start Menu→Setting→Control Panel. In the Control Panel, double click on the Network Connections (Network and Dialup Connections in Windows 2000) icon.
- Double click the Local Area Connection icon. Under the General Tab, click the Properties button.
- Select Internet Protocol (TCP/IP) and click the Properties button.
- Under the General Tab, make sure that the Obtain an IP address automatically and Obtain DNS Server Address Automatically options are selected. If they are not selected, select them and click the OK button. This will make your IP dynamic, allowing it to change each time you connect/disconnect.



D.2 Windows 95/98/98SE/Me

- Click on Start Menu→Settings→ Control Panel. In the Control Panel, double-click the Network icon.
- Select the TCP/IP for the ADSL Router (i.e. TCP/IP→Conexant USB Network Adapter) and click the Properties button.
- Select the IP Address tab and click Obtain an IP address automatically.
- Click OK to close TCP/IP Properties and then click OK to close Network.



D.3 AC OS (7.6.1 or higher)

- Select Control Panels from the Apple Menu and open the TCP/IP Control Panel.
- Choose the Connect via Ethernet option.
- Select Configure using DHCP Server option.
- Close and Save.

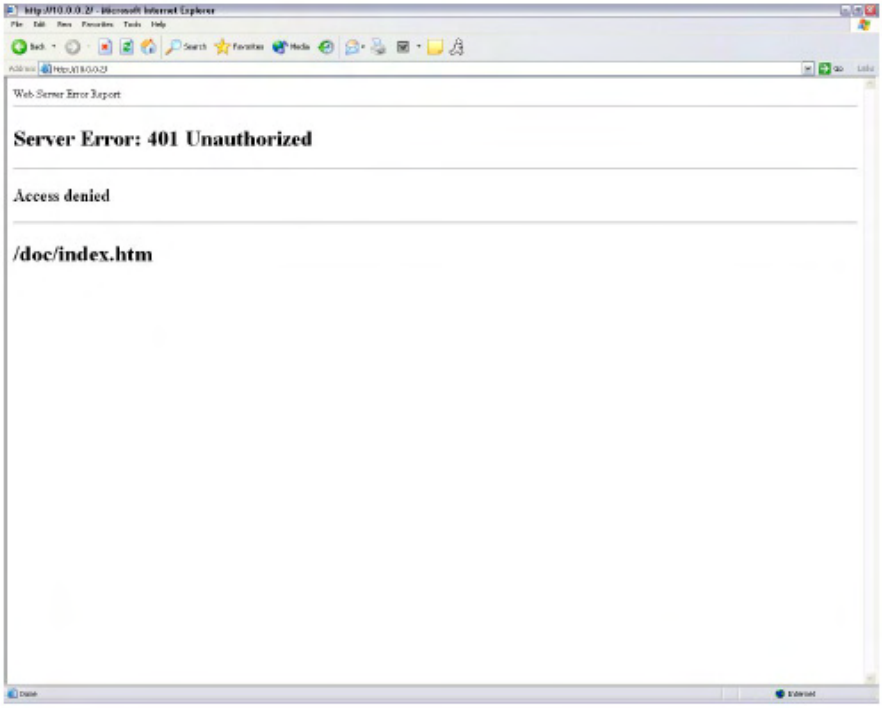
D.4 MAC OS X

- Launch System Preferences from the Apple Menu and select the Network Preference Pane.
- Choose Show: Built-in Ethernet.
- Click on the TCP/IP tab.
- Choose Configure: Using DHCP.
- Quit System Preferences.

Appendix E Common Error Messages

This Appendix provides a library of common error messages, explaining how each one is obtained and how to keep them error from reoccurring.

1. Server Error: 401 Unauthorized – Access Denied



This error occurs when an Invalid Login attempt is made. This is caused by an invalid user name and/or password.

2. Server Error: 403 Forbidden – Access Denied

This error occurs when the standard user account (non-admin) attempts to load pages under the Admin Privilege section.

This error message can vary, depending on the access attempt. In the variations, the bottom line **/doc/wan.htm** may be replaced with something else.

Appendix F Glossary

The Glossary provides an explanation of terms and acronyms discussed in this user guide.

AP : Access Point: A station that transmits and receives data in a WLAN (Wireless Local Area Network). An access point acts as a bridge for wireless devices into a LAN.

ATM : Asynchronous Transfer Mode: A method of transfer in which data is organized into 53-byte cell units. ATM cells are processed asynchronously in relation to other cells.

BC : Broadcast: Communication in which a sender transmits to everyone in the network.

BER : Bit Error Rate: Percentage of Bits that contain errors relative to the total number of bits transmitted.

Bridge : A device that connects two networks and decides which network the data should go to.

Bridge Mode : Bridge Mode is used when there is one PC connected to the LAN-side Ethernet or USB port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet or USB) side, i.e., to store and forward.

CBR : Constant Bit Rate: A constant transfer rate that is ideal for streaming (executing while still downloading) data, such as audio or video files.

Cell : A unit of transmission in ATM, consisting of a fixed-size frame containing a 5-octet header and a 48-octet payload.

CHAP : Challenge Handshake Authentication Protocol: Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

CLP : Cell Loss Priority: ATM cells have two levels of priority, CLP0 and CLP1. CLP0 is of higher priority, and in times of high traffic congestion, CLP1 error cells may be discarded to preserve the Cell Loss Ratio of the CLP0 cells.

CO : Central Office: In a local loop, a Central Office is where home and office phone lines come together and go through switching equipment to connect them to other Central Offices. The distance from the Central Office determines whether or not an ADSL signal can be supported in a given line.

CPE : Customer Premises Equipment. This specifies equipment on the customer, or LAN, side.

CRC : Cyclic Redundancy Checking: A method for checking errors in a data transmission between two computers. CRC applies a polynomial function (16 or 32-bit) to a block of data. The result of that polynomial is appended to the data transmission. Upon receipt, the destination computer applies the same polynomial to the block of data. If the host and destination computer share the same result, the transmission was successful. Otherwise, the sender is notified to re-send the data block.

DHCP : Dynamic Host Configuration Protocol: A communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP can lease and IP address or provide a permanent static address to those computers who need it (servers, etc.).

DMZ : Demilitarized Zone: A computer Host or network that acts as a neutral zone between a private network and a public network. A DMZ prevents users outside of the private network from getting direct access to a server or any computer within the private network. The outside user sends requests to the DMZ, and the DMZ initiates sessions in the public network based on these requests. A DMZ cannot

initiate a session in the private network, it can only forward packets to the private network as they are requested.

DNS : Domain Name System: A method to locate and translate Domain Names into Internet Protocol (IP) addresses, where a Domain Name is a simple and meaningful name for an Internet address.

DSL : Digital Subscriber Line: A technology that provides broadband connections over standard phone lines.

DSLAM : Digital Subscriber Line Access Multiplexer: Using multiplexing techniques, a DSLAM receives signals from customer DSL lines and places the signals on a high-speed backbone line. DSLAMs are typically located at a telephone company's CO (Central Office).

Encapsulation : The inclusion of one data structure within another. For example, packets can be encapsulated in an ATM frame during transfer.

FEC : Forward Error Correction: An error correction technique in which a data packet is processed through an algorithm that adds extra error correcting bits to the packet. If the transmitted message is received in error, these bits are used to correct the errored bits without retransmission.

Firewall : A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Fragmentation : Breaking a packet up into smaller packets that is caused either by the transmission medium being unable to support the original size of the packet or the receiving computer not being able to receive a packet of that size. Fragmentation occurs when the sender's MTU is larger than the receiver's MRU.

FTP : File Transfer Protocol. A standardized internet protocol which is the simplest way to transfer files from one computer to another over the internet. FTP uses the Internet's TCP/IP protocols to function.

Full Duplex : Data transmission can be transmitted and received on the same signal medium and at the same time. Full Duplex lines are bidirectional.

G.dmt : Formally G.992.1, G.dmt is a form of ADSL that uses Discrete MultiTone (DMT) technology. G.dmt incorporates a splitter in its design.

G.lite : Formally G.992.2, G.lite is a standard way to install ADSL service. G.lite enables connections speeds up to 1.5 Mbps downstream and 128 kbps upstream. G.lite does not need a splitter at the user end because splitting is preformed at the remote end (telephone company).

Gateway : A point on the network which is an entrance to another network. For example, a router is a gateway that connects a LAN to a WAN.

Half Duplex : Data transmission can be transmitted and received on the same signal medium, but not simultaneously. Half Duplex lines are bidirectional.

HEC : Headed Error Control: ATM error checking by using a CRC algorithm on the fifth octet in the ATM cell header to generate a check character. Using HEC, either a single bit error in the header can be corrected or multiple bit errors in the header can be detected.

HNP : Home Network Processor

Host : In context of Internet Protocol, a host computer is one that has full two way access to other computers on the Internet.

IAD : Integrated Access Device: A device that multiplexes and demultiplexes communications in the CPE onto and out of a single telephone line for transmission to the CO.

IP : Internet Protocol: The method by which information is sent from one computer to another through the Internet. Each of these host computers have a unique IP address which distinguishes it from all the other computers on the internet. Each packet of data sent includes the sender's IP address and the receiver's IP address.

LAN : Local Area Network: A group of computers, typically covering a small geographic area, that share devices such as printers, hard disk drives, scanners, and optical drives. Computers in a LAN typically share an internet connection through some sort of router that connects the computers to a WAN.

LLC : Logical Link Control: Provides an interface point to the MAC sublayer. LLC Encapsulation is needed when several protocols are carried over the same Virtual Circuit.

MAC Address : Media Access Control Address: A unique hardware number on a computer or device that identifies it and relates it to the IP address of that device.

MC : Multicast: Communication involving a single sender and multiple specific receivers in a network.

MRU : Maximum Receive Unit: MRU: Maximum Receive Unit (MRU) is the largest size packet that can be received by the modem. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MSS : Maximum Segment Size: The largest size of data that TCP will send in a single, unfragmented IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their Maximum Segment Size during the TCP connection handshake.

MTU : Maximum Transmission Unit: The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

NAPT : Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

NAT : Network Address Translation: The translation of an IP address of one network to a different IP address known by another network. This gives an outside (WAN) network the ability to distinguish a device on the inside (LAN) network, as the inside network has a private set of IP address assigned by the DHCP server not known to the outside network.

PAP : Password Authentication Protocol: An authentication protocol in which authorization is done through a user name and password.

PDU : Protocol Data Unit: A frame of data transmitted through the data link layer 2.

Ping : Packet Internet Groper: A utility used to determine whether a particular device is online or connected to a network by sending test packets and waiting for a response.

PPP : Point-to-Point Protocol: A method of transporting and encapsulating IP packets between the user PC and the ISP. PPP is full duplex protocol that is transmitted through a serial interface.

Proxy : A device that closes a straight connection from an outside network (WAN) to an inside network (LAN). All transmissions must go through the proxy to get into or out of the LAN. This makes the internal addresses of the devices in the LAN private.

PVC : Permanent Virtual Circuit: A software defined logical connection in a network; A Virtual Circuit that is permanently available to the user.

RIP : Routing Information Protocol: A management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge.

RIPv1 : RIP Version 1: One of the first dynamic routing protocols introduced used in the internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.

RIPv2 : RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to broadcasting.

Router Mode : Router Mode is used when there is more than one PC connected to the LAN-side Ethernet and/or USB port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address.

SNAP : SubNetwork Attachment Point.

SNMP : Simple Network Management Protocol: Used to govern network management and monitor devices on the network. SNMP is formally described in RFC 1157.

SNR : Signal-to-Noise Ratio: Measured in decibels, SNR is a calculated ratio of signal strength to background noise. The higher this ratio, the better the signal quality.

Subnet Mask : Short for SUBNETwork Mask, subnet mask is a technique used by the IP protocol to filter messages into a particular network segment, called a subnet. The subnet mask consists of a binary pattern that is stored in the client computer, server, or router. This pattern is compared with the incoming IP address to determine whether to accept or reject the packet.

TCP : Transfer Control Protocol: Works together with Internet Protocol for sending data between computers over the Internet. TCP keeps track of the packets, making sure that they are routed efficiently.

TFTP : Trivial File Transfer Protocol: A simple version of FTP protocol that has no password authentication or directory structure capability.

Trellis Code : An advanced method of FEC (Forward Error Correction). When enabled, it makes for better error checking at the cost of slower packet transmission. Setting Trellis Code to Disabled will cause increased packet transmission with decreased error correction.

TTL : Time To Live: A value in an IP packet that indicates whether or not the packet has been propagating through the network too long and should be discarded.

UBR : Unspecified Bit Rate: A transfer mode that is usually used in file transfers, email, etc. UBR can vary depending on the data type.

USB : Universal Serial Bus: A standard interface between a computer and a peripheral (printer, external drives, digital cameras, scanners, network interface devices, modems, etc.) that allows a transfer rate of 12Mbps.

UDP : User Datagram Protocol: A protocol that is used instead of TCP when reliable delivery is not required. Unlike TCP, UDP does not require an acknowledgement (handshake) from the receiving end. UDP sends packets in one-way transmissions.

VBR-nrt : Variable Bit Rate – non real time: With VBR-nrt, cell transfer is variable upon certain criteria.

VC : Virtual Circuit: A virtual circuit is a circuit in a network that appears to be a physically discrete path, but is actually a managed collection of circuit resources that allocates specific circuits as needed to satisfy traffic requirements.

VCI : Virtual Channel Identifier: A virtual channel identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel.

VC-Mux : Virtual Circuit based Multiplexing: In VC Based Multiplexing, the interconnect protocol of the carried network is identified implicitly by the VC (Virtual Circuit) connecting the two ATM stations (each protocol must be carried over a separate VC).

VPI : Virtual Path Identifier: Virtual path for cell routing indicated by an eight bit field in the ATM cell header.

WAN : Wide Area Network: A WAN covers a large geographical area. A WAN is consisted of LANs and the Internet is consisted of WANs.